FortiAnalyzer - Administration Guide

VERSION 5.0.13

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

2016-07-14

FortiAnalyzer 5.0.13 Administration Guide

05-5013-187572-20160714

TABLE OF CONTENTS

Change Log **9**
Introduction **10**
Feature support 10
FortiAnalyzerdocumentation 11
Scope 11
Entering FortiAnalyzer configuration data 11
Entering text strings (names) 12
Selecting options from a list 12
Enabling or disabling options 12
What's New in FortiAnalyzer 5.0.13 ..... **13**
FortiAnalyzer 5.0.13 13
FortiAnalyzer 5.0.12 13
FortiAnalyzer 5.0.11 13
FortiAnalyzer 5.0.10 13
Logging 13
Reports 13
System settings 13
FortiAnalyzer 5.0.9 13
FortiAnalyzer 5.0.8 14
FortiView 14
Reports 14
Logging 14
Other 14
FortiAnalyzer 5.0.7 14
Event management 14
FortiView 14
Logging 14
Reports 15
Other 15
FortiAnalyzer 5.0.6 15
Charts 15
Reports 15
Logging 16
Event management 16

Other 16
FortiAnalyzer 5.0.5 16
Cover page customization 16
Report text element customization 16
SIP/SCCP datasets 16
Summary of enhancements: 17
Logging 17
Other 17
FortiAnalyzer5.0.4 17
Summary of enhancements: 17
FortiAnalyzer5.0.3 18
RAID management page 18
Pre-processing logic of ebtime 18
FortiMail/FortiWeb logging and reporting support 18
Event management tab 19
FortiAnalyzerVM support for Microsoft Hyper-V Server 19
Summary of enhancements 19
FortiAnalyzer 5.0.2 19
FortiClient logging 19
Backup/restore logs and reports 19
CLI command branch change 20
XML web service support 20
Summary of enhancements 20
FortiAnalyzer 5.0.1 21
Key Concepts 22
Administrative domains 22
Operation modes 22
Feature comparison between analyzer and collector mode 23
Analyzer mode 23
Analyzer and collector mode 24
Log storage 26
Workflow 26
GUI 28
System requirements 28
Web browser support 28
Screen resolution 28
Connecting to the GUI 28
GUI overview 29
GUI configuration 30
Language support 31
Administrative access 32
Restricting access by trusted hosts 33

Idle timeout 33
Reboot and shutdown the FortiAnalyzer unit 34
Administrative Domains 35
Adding an ADOM 35
Assigning devices to an ADOM 37
Assigning administrators to an ADOM 38
ADOM device modes 38
Device Manager 39
Devices 40
Devices and VDOMs 41
FortiGate HA clusters 45
Unregistered devices 47
Device reports 47
Log forwarding 47
Disk space allocation 49
Log arrays in FortiAnalyzer v5.0.7 and later 49
System Settings 50
Dashboard 51
Customizing the dashboard 53
System Information widget 53
License Information widget 58
Unit Operation widget 59
System Resources widget 59
Alert Messages Console widget 61
CLI Console widget 62
Log Receive Monitor widget 63
Logs/Data Received widget 63
Statistics widget 64
Insert Rate vs Receive Rate widget 65
Log Insert Lag Time widget 65
All ADOMs 66
RAID management 68
Supported RAID levels 69
RAID disk status 72
Hot swapping hard disks 72
Adding new disks 73
Network 74
Network interfaces 75
Static routes 76
Diagnostic tools 77
Admin 77
Monitoring administrator sessions 78

Administrator 79
Profile 82
Remote authentication server 85
Administrator settings 89
Configure two-factor authentication for administrator login 91
Certificates 96
Local certificates 96
CA certificates 99
Certificate revocation lists 100
Event log 100
Task monitor 103
Advanced 104
SNMP v1/v2c 105
Mail server 109
Syslog server 109
Meta fields 110
Device log settings 111
File management 112
Advanced settings 113
FortiView 114
FortiView 114
Top Sources 114
Top Applications 117
Top Destinations 119
Top Web Sites 121
Top Threats 124
Top Cloud Applications 126
Log view 128
Viewing log messages 130
Customizing the log view 132
Custom views 135
Searching log messages 136
Download log messages 137
Log arrays 137
Log details 138
Archive 139
Browsing log files 139
FortiClient logs 141
Configuring rolling and uploading of logs 142
Event Management 144
Events 144
Event details 145

Acknowledge events 147
Event handler 147
Manage event handlers 152
Reports 156
Reports 156
Configuration tab 159
Advanced settings tab 160
View report tab 163
Report layouts 165
Workspace settings 165
Sections 166
Elements 168
Chart library 173
Custom chart wizard 174
Managing charts 177
Macro library 180
Managing macros 181
Report calendar 184
Advanced 185
Dataset 185
Output profile 189
Language 191
Appendix A - Report Templates 193
FortiGate reports 193
FortiMail reports 203
FortiWeb report 204
FortiCache report 205
Appendix B - Charts, Datasets, & Macros 206
FortiGate 206
Predefined charts 206
Predefined datasets 222
Predefined macros 234
FortiMail 236
Predefined charts 236
Predefined datasets 238
FortiWeb 240
Predefined charts 240
Predefined datasets 241
FortiCache 242
Predefined charts 242
Predefined datasets 243
Appendix C - Port Numbers 244

Appendix D - Maximum Values Matrix **246**
Appendix E - SNMP MIB Support **248**
SNMP MIB Files 248
FORTINET-CORE-MIB 248
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB 257

Change Log

Date	Change Description
2012-11-20	Initial release.
2013-01-14	Update for FortiAnalyzer 5.0.1.
2013-04-02	Updated for FortiAnalyzer 5.0.2.
2013-04-24	Updated log rolling and uploading configuration and firmware update instructions.
2013-05-29	Updated introductory feature list.
2013-07-16	Updated for FortiAnalyzer 5.0.3.
2013-09-13	Updated for FortiAnalyzer 5.0.4.
2013-09-20	Added information on device disk log quota.
2013-11-13	Updated for FortiAnalyzer 5.0.5.
2014-01-30	Updated for FortiAnalyzer 5.0.6.
2014-02-24	Corrected typographic issues.
2014-03-10	Removed FortiAnalyzer supported devices from Introduction chapter. For more information, see the product data sheet.
2014-07-09	Updated for FortiAnalyzer 5.0.7.
2014-10-07	Updated for FortiAnalyzer 5.0.8.
2014-10-20	Updated for FortiAnalyzer 5.0.9.
2015-01-30	Updated for FortiAnalyzer 5.0.10.
2015-06-11	Updated for FortiAnalyzer 5.0.11.
2016-07-14	Updated for FortiAnalyzer 5.0.13.

Introduction

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

FortiAnalyzer offers enterprise class features to identify threats, while providing the flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements, while aggregating logs in a hierarchical, tiered logging topology.

You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Logging	FortiView	Event Management	Reports
FortiGate	✔	✔	✔	✔
FortiCache	✔			✔
FortiCarrier	✔	✔	✔	✔
FortiClient	✔			
FortiMail	✔			✔
FortiSandbox	✔			
FortiWeb	✔			✔
Syslog	✔			

For more information on supported platforms, see the FortiAnalyzer Release Notes.

FortiAnalyzerdocumentation

The following FortiAnalyzer product documentation is available:

- *FortiAnalyzer Administration Guide*
  This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- *FortiAnalyzer device QuickStart Guides*
  These documents are included with your FortiAnalyzer system package. Use this document to install and begin working with the FortiAnalyzer system and FortiAnalyzer GUI.
- *FortiAnalyzer Online Help*
  You can get online help from the FortiAnalyzer GUI. FortiAnalyzer online help contains detailed procedures for using the FortiAnalyzer GUI to configure and manage FortiGate units.
- *FortiAnalyzer CLI Reference*
  This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for all FortiAnalyzer CLI commands.
- *FortiAnalyzer Release Notes*
  This document describes new features and enhancements in the FortiAnalyzer system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiAnalyzer VM Install Guide*
  This document describes installing FortiAnalyzer VM in your virtual environment.

Scope

This document describes how to use the GUI to set up and configure a FortiAnalyzer unit. It assumes you have already successfully installed the FortiAnalyzer unit by following the instructions in your unit's QuickStart guide.

At this stage:

- You have administrative access to the GUI and/or Command Line Interface (CLI), and
- The FortiAnalyzer unit can connect to the GUI and CLI.

This document explains how to use the GUI to:

- Maintain the FortiAnalyzer unit, including backups
- Configure basic settings, such as system time, DNS settings, administrator passwords, and network interfaces
- Configure advanced features, such as adding devices, DLP archiving, logging, and reporting.

This document does not cover commands for the Command Line Interface (CLI). For information on the CLI, see the FortiAnalyzer CLI Reference.

Entering FortiAnalyzer configuration data

The configuration of a FortiAnalyzer unit is stored as a series of configuration settings in the FortiAnalyzer configuration database. Use the GUI or CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a report chart, administrative user, and so on. You can enter any character in a FortiAnalyzer configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than), and > (greater than)

Selecting options from a list

If a configuration field can only contain one of a number of selected options, the GUI and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI, you must spell the selection name correctly.

Enabling or disabling options

If a configuration field can only be on or off (enabled or disabled), the GUI shows a check box or other control that can only be enabled or disabled. From the CLI, you can set the option to `enable` or `disable`.

What's New in FortiAnalyzer 5.0.13

FortiAnalyzer 5.0 includes the following new features and enhancements. Always review all sections in the *FortiAnalyzer Release Notes* prior to upgrading your device.

FortiAnalyzer 5.0.13

FortiAnalyzer 5.0.13 includes no new features.

FortiAnalyzer 5.0.12

FortiAnalyzer 5.0.12 includes no new features.

FortiAnalyzer 5.0.11

FortiAnalyzer 5.0.11 includes no new features.

FortiAnalyzer 5.0.10

Logging

- Progress bar displays the status of the SQL log database rebuild

Reports

- Report grouping

System settings

- New widgets: Insert Rate vs Receive Rate and Log Insert Lag Time.

FortiAnalyzer 5.0.9

There are no new features or enhancements in FortiAnalyzer 5.0.9.

FortiAnalyzer 5.0.8

FortiAnalyzer 5.0.8 includes the following new features and enhancements.

FortiView

- Cloud user view and cloud application drilldown view

Reports

- FortiCache reporting support

Logging

- FortiSandbox logging support
- Log forwarding in Analyzer mode

Other

- Tool for validating custom datasets
- Auto discover FortiGate HA clusters
- Support FortiGate HA clusters for device registration, logging, and reporting
- Added FG-92D and FWF-92D support
- Added FG-1000D support
- Added FG-5001D support
- Added FGR-60D support
- Added FGV-70D4 support

FortiAnalyzer 5.0.7

FortiAnalyzer 5.0.7 includes the following new features and enhancements.

Event management

- Event Handler for local FortiAnalyzer event logs

FortiView

- New FortiView module

Logging

- Updated compact log v3 format from FortiGate
- Explicit proxy traffic logging support

Reports

- Improvements to report configuration
- Improvements to the Admin and System Events Report template
- Improvements to the VPN Report template
- Improvements to the Wireless PCI Compliance Report template
- Improvements to the Security Analysis Report template
- New Intrusion Prevention System (IPS) Report template
- New Detailed Application Usage and Risk Report template
- New FortiMail Analysis Report template
- New pre-defined Application and Websites report templates
- Macro library support
- Option to display or upload reports in HTML format

Other

- Syslog server logging support

FortiAnalyzer 5.0.6

FortiAnalyzer 5.0.6 includes the following new features and enhancements.

Charts

- Chart improvements:
  - Charts in the *Chart Library* are listed in alphabetical order by default.
  - Charts have been renamed for improved usability.
  - The chart library and database have been improved.
- New charts
  - Botnet activity charts: Four new charts have been added for Botnet activity.
  - Site-to-Site VPN charts.

Reports

The following reports have been improved:

- Bandwidth and Applications Report
- Security Analysis report
- Threat Report
- User Report
- Web Usage Report

Logging

- Improved FortiAnalyzer insert rate performance
- Log filter improvements
- When the FortiAnalyzer device is in collector mode, you can configure log forwarding in the *Device Manager* tab.

Event management

- FortiOS v4.0 MR3 logs are now supported.
- Support subject customization of alert email.

Other

- Automatically delete log files, quarantined files, reports, and content archive files older than a specified time period.
- FortiAnalyzer VM supports up to 12 virtual disks (LVM).

FortiAnalyzer 5.0.5

FortiAnalyzer 5.0.5 includes the following new features and enhancements.

Cover page customization

You can now customize the report cover page images and text in the report template page.

Report text element customization

You can now customize the report text element. You can apply bold and italics to text, indent text, and create both bulleted and numbered lists.

SIP/SCCP datasets

The following datasets have been added to FortiAnalyzer for SIP and SCCP support:

- appctrl-Top-Block-SCCP-Callers
- appctrl-Top-Blocked-SCCP-Callers-by-Blocking-Criteria
- content-Count-Total-SCCP-Call-Registrations-by-Hour-of-Day
- content-Count-Total-SCCP-Calls-Duration-by-Hour-of-Day
- content-Count-Total-SCCP-Calls-per-Status
- appctrl-Top-Blocked-SIP-Callers
- appctrl-Top-Blocked-SIP-Callers-by-Blocking-Criteria
- content-Count-Total-SIP-Call-Registrations-by-Hour-of-Day
- content-Count-Total-SIP-Calls-per-Status
- content-Dist-Total-SIP-Calls-by-Duration

Summary of enhancements:

The following is a list of enhancements in FortiAnalyzer 5.0.5.

- Reports
- SIP/SCCP datasets
- Added Spyware, Adware, and other predefined charts to the Threat Report
- Added an *OR* option to the report filter
- Cover page customization

Logging

- Added support to upload logs to multiple rolling servers
- Configurable FortiAnalyzer option and device filters for Log Forwarding and Aggregation
- Log Search enhancements

Other

- Added System Charts and Custom Charts checkboxes to filter out predefined charts or customized charts.
- Download FortiGuard Databases for more detailed reports

FortiAnalyzer5.0.4

FortiAnalyzer 5.0.4 includes the following new features and enhancements.

Summary of enhancements:

The following is a list of enhancements in FortiAnalyzer 5.0.4.

Reports

- Option to remove the FortiAnalyzer report cover page
- Generate per user reports (setup via XML)
- Chart builder wizard
- Predefined report template for custom application report
- Predefined report template for threat activity
- Change the background color, text color, text size, and text style in reports
- Format text areas and headers in report
- Report cover page customization
- Usability enhancements for reports
- New report templates

Logging

- Log forward in CEF format
- SQL index performance optimizations and enhanced log search support
- Import logs from a remote FTP/SCP/SFTP server
- Configure up to three log rolling upload servers

Other

- Export and import image files along with report DAT files
- Event Management extensions and enhancements
- New system dashboard widgets: Statistics, Logs/Data Received, Log Receive Monitor

FortiAnalyzer5.0.3

FortiAnalyzer 5.0.3 includes the following new features and enhancements.

RAID management page

A RAID Management menu item replaces the existing RAID Monitor widget. This enhancement extends the existing RAID monitoring capabilities allowing you to perform simple RAID management tasks such as add, remove, or replace disks and reconfigure RAID levels.

This page provides a summary of RAID information including the RAID level configured, status, disk space usage, and disk status. When hovering your mouse cursor over each disk, a pop-up window provides the disk number, model, firmware, RAID level, capacity, and disk status.

You can use the right-click menu to repair, add, or delete disks.

Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:

Traffic logs with `logid` of `13` or `2`, when `logid == 13`, `hostname` must not be empty. The `service` field should be either `HTTP`, `80/TCP` or `443/TCP`.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.

FortiMail/FortiWeb logging and reporting support

FortiAnalyzer v5.0.3 or later supports FortiMail and FortiWeb logging and reporting. ADOMs must be enabled on FortiAnalyzer before these devices can be added. FortiMail and FortiWeb are log triggered devices. Once configured to log to the FortiAnalyzer they will be displayed in the unregistered device list. Upon promoting the device to the DVM table, it will be added to the respective default ADOM.

FortiMail and FortiWeb devices cannot be added using the Add Model Device wizard.

Event management tab

In Event Management you can configure events based on logging filters. You can select to send the event to an email address, SNMP server, or syslog server. Events can be configured per device or for all devices. You can create events for FortiGate, FortiCarrier, FortiMail, and FortiWeb devices.

FortiAnalyzerVM support for Microsoft Hyper-V Server

FortiAnalyzer VM now supports Microsoft Hyper-V Server 2008 R2 and 2012 virtualization environments.

Summary of enhancements

The following is a list of enhancements in FortiAnalyzer 5.0.3:

- Log search
- Device storage and log management
- RAID management page
- Report GUI enhancements
- Merge event log based charts to the default report
- Chart level filters
- Report filter improvements
- Event management tab
- FortiMail logging and reporting support
- FortiWeb logging and reporting support
- VM support for Microsoft Hyper-V Server
- Added support for real-time syslog forwarding over TCP connections
- Import and export report templates
- Web Filter report template
- WiFi Network Summary report template

FortiAnalyzer 5.0.2

FortiAnalyzer 5.0.2 includes the following new features and enhancements.

FortiClient logging

Support has been added to FortiAnalyzer to allow you to log FortiClient endpoint traffic. FortiClient logs are stored under a single device object. This feature requires FortiClient 5.0.2 or later.

Backup/restore logs and reports

The following CLI commands have been added to FortiAnalyzer v5.0.2 to allow you to backup and restore logs and reports:

- `execute backup logs`: Backup device logs to a specified server.
- `execute backup logs-only`: Backup device logs only to a specified server.
- `execute backup reports`: Backup reports to a specified server.
- `execute restore logs`: Restore device logs and DLP archives from a specified server.
- `execute restore logs-only`: Restore device logs from a specified server.
- `execute restore reports`: Restore reports from a specified server.

CLI command branch change

In FortiAnalyzer 5.0.2, the `fmsystem` and `fasystem` CLI branches have been merged into the `system` branch.

XML web service support

FortiAnalyzer web services has been enhanced to support SQL reporting. The following APIs are now supported in SQL:

- runFazReport
- getFazGeneratedReport
- listFazGeneratedReports
- getFazArchive
- removeFazArchive
- getSystemStatus
- getFazConfig
- setFazConfig
- searchFazLog

To download the Web Server Description Language (WSDL) file on your FortiAnalyzer, go to *System Settings* > *Advanced* > *Advanced Settings*. Select the download WSDL file icon to save the file to your management computer.

Summary of enhancements

The following is a list of enhancements in FortiAnalyzer v5.0.2:

- Group reports
- Backup/restore logs and reports
- CLI command branch change
- Client reputation report template
- FortiClient logging
- Predefined charts and datasets for wireless
- Reliable FortiAnalyzer logging
- Report template updates
- SNMP support and management information base (MIB) updates
- SQL query tool in the GUI
- *System Resources* widget enhancement
- XML web service support

FortiAnalyzer 5.0.1

FortiAnalyzer 5.0.1 includes the following new features and enhancements:

- Added support for IPv6 networking
- Auto-generate log fields
- Certificate compatibility with FortiGate
- Dataset improvements
- GTP log compatibility
- Improved Collector and Analyzer modes
- Log Aggregation (Collector mode)
- Multiple concurrent running reports
- New DVM table
- New FortiAnalyzer VM licensing model
- Support OU for the report LDAP filter

Key Concepts

This chapter defines basic FortiAnalyzer concepts and terms.

If you are new to FortiAnalyzer, this chapter can help you to quickly understand this document and your FortiAnalyzer platform.

This topic includes:

- Administrative domains
- Operation modes
- Log storage
- Workflow

Administrative domains

Administrative domains (ADOMs) enable the `admin` administrator to constrain other FortiAnalyzer unit administrators access privileges to a subset of devices in the device list. For Fortinet devices with virtual domains (VDOMs), ADOMs can further restrict access to only data from a specific device's VDOM.

Enabling ADOMs alters the structure of and the available functions in the GUI and CLI, according to whether or not you are logging in as the `admin` administrator, and, if you are not logging in as the `admin` administrator, the administrator account's assigned access profile. See System Information widget on page 53 for information on enabling and disabling ADOMs.

For information on working with ADOMs, See Administrative Domains on page 35. For information on configuring administrators and administrator settings, See Admin on page 77

ADOMs must be enabled to support FortiCarrier, FortiMail, FortiWeb, FortiCache, and FortiSandbox logging and reporting. See Administrative Domains on page 35.

Operation modes

The FortiAnalyzer unit has two operation modes:

- *Analyzer*: The default mode that supports all FortiAnalyzer features. This mode used for aggregating logs from one or more log collectors. In this mode, the log aggregation configuration function is disabled.
- *Collector*: The mode used for saving and uploading logs. For example, instead of writing logs to the database, the collector can retain the logs in their original (binary) format for uploading. In this mode, the report function and some functions under the System Settings tab are disabled.

The analyzer and collector modes are used together to increase the analyzer's performance. The collector provides a buffer to the FortiAnalyzer by off-loading the log receiving task from the analyzer. Since log collection from the connected devices is the dedicated task of the collector, its log receiving rate and speed are maximized.

The mode of operation that you choose will depend on your network topology and individual requirements. For information on how to select an operation mode, see Changing the operation mode on page 57.

Feature comparison between analyzer and collector mode

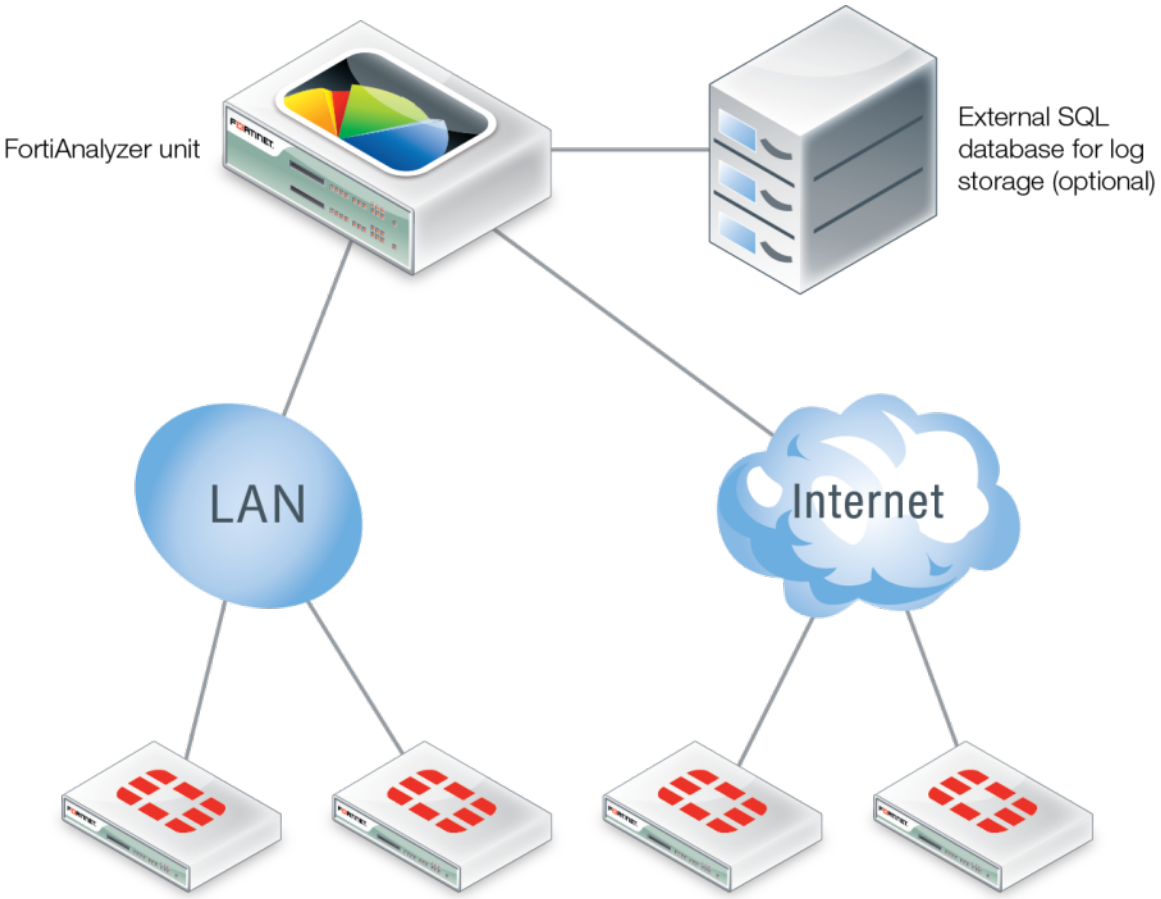
The operation mode options have been simplified to two modes, Analyzer and Collector. Standalone mode has been removed.

	Analyzer Mode	Collector Mode
Event Management	Yes	No
Monitoring	Yes	No
Reporting	Yes	No
FortiView/Log View	Yes	Yes
Device Manager	Yes	Yes
System Settings	Yes	No
Log Forwarding	Yes	Yes

Analyzer mode

The analyzer mode is the default mode that supports all FortiAnalyzer features. If your network log volume does not compromise the performance of your FortiAnalyzer unit, you can choose this mode.

The below illustrations shows the network topology of the FortiAnalyzer unit in analyzer mode.



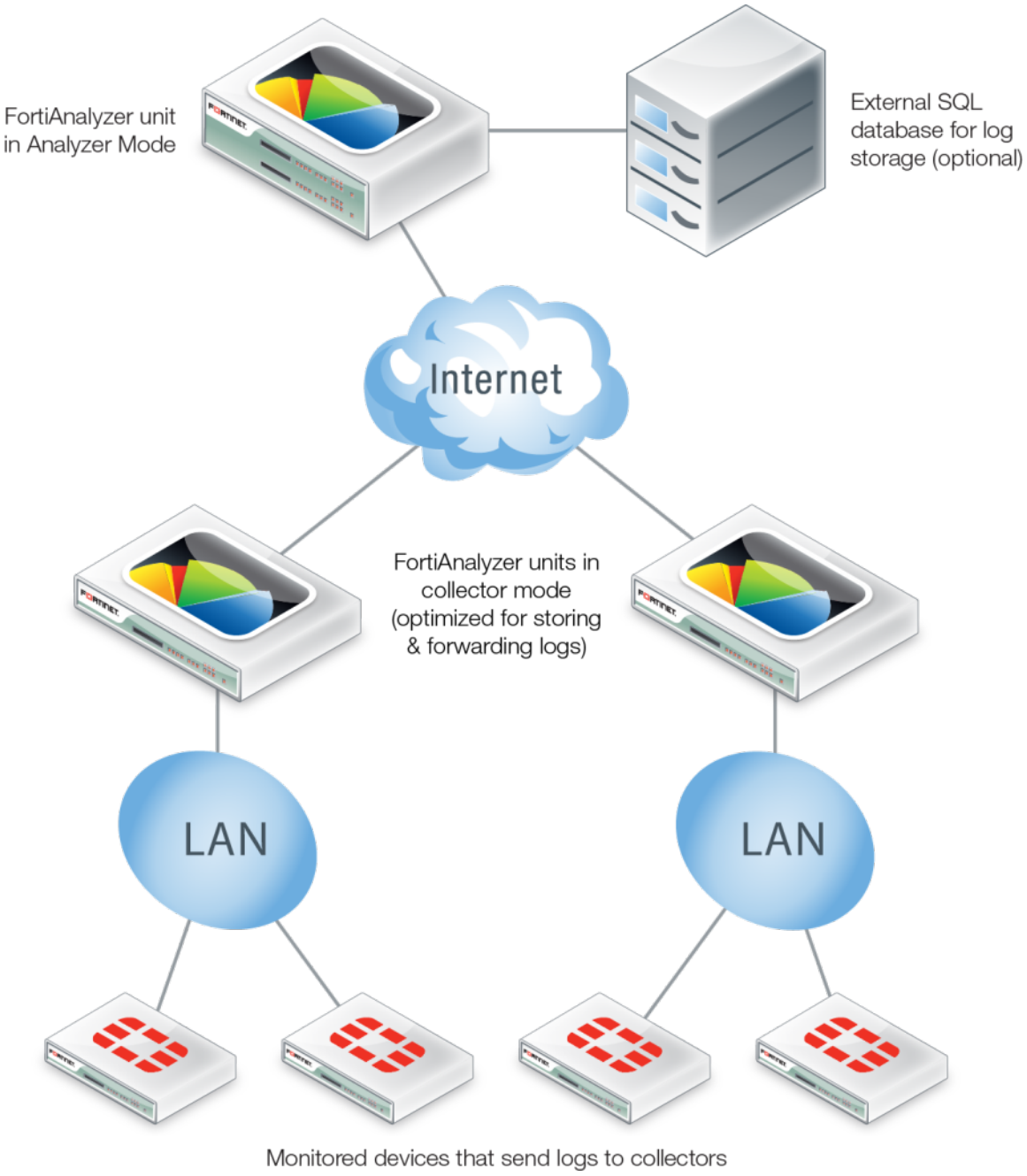
Monitored devices that send logs to the FortiAnalyzer unit for analyzing and reporting.

Analyzer and collector mode

The analyzer and collector modes are used together to increase the analyzer's performance. The collector provides a buffer to the analyzer by off-loading the log receiving task from the analyzer. Since log collection from the connected devices is the dedicated task of the collector, its log receiving rate and speed are maximized.

In most cases, the volume of logs fluctuates dramatically during a day or week. You can deploy a collector to receive and store logs during the high traffic periods and transfer them to the analyzer during the low traffic periods. As a result, the performance of the analyzer is guaranteed as it will only deal with log insertion and reporting when the log transfer process is over.

As illustrated below: company A has two remote branch networks protected by multiple FortiGate units. The networks generate large volumes of logs which fluctuate significantly during a day. It used to have a FortiAnalyzer 4000B in analyzer mode to collect logs from the FortiGate units and generate reports. To further boost the performance of the FortiAnalyzer 4000B, the company deploys a FortiAnalyzer 400C in collector mode in each branch to receive logs from the FortiGate units during the high traffic period and transfer bulk logs to the FortiAnalyzer 4000B during the low traffic period.



To set up the analyzer/collector configuration:

1. On the FortiAnalyzer unit, go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Operation Mode* field, select *Change*.
3. Select *Analyzer* in the *Change Operation Mode* dialog box.
4. Select *OK*.
5. On the first collector unit, go to *System Settings* > *Dashboard*.
6. In the *System Information* widget, in the *Operation Mode* field, select *Change*.
7. Select *Collector* from the *Change Operation Mode* dialog box.

8. Select *OK*.
   For more information on configuring log forwarding, see Log forwarding on page 47.

Log storage

The FortiAnalyzer unit supports Structured Query Language (SQL) logging and reporting. The log data is inserted into the SQL database for generating reports. Both local and remote SQL database options are supported.

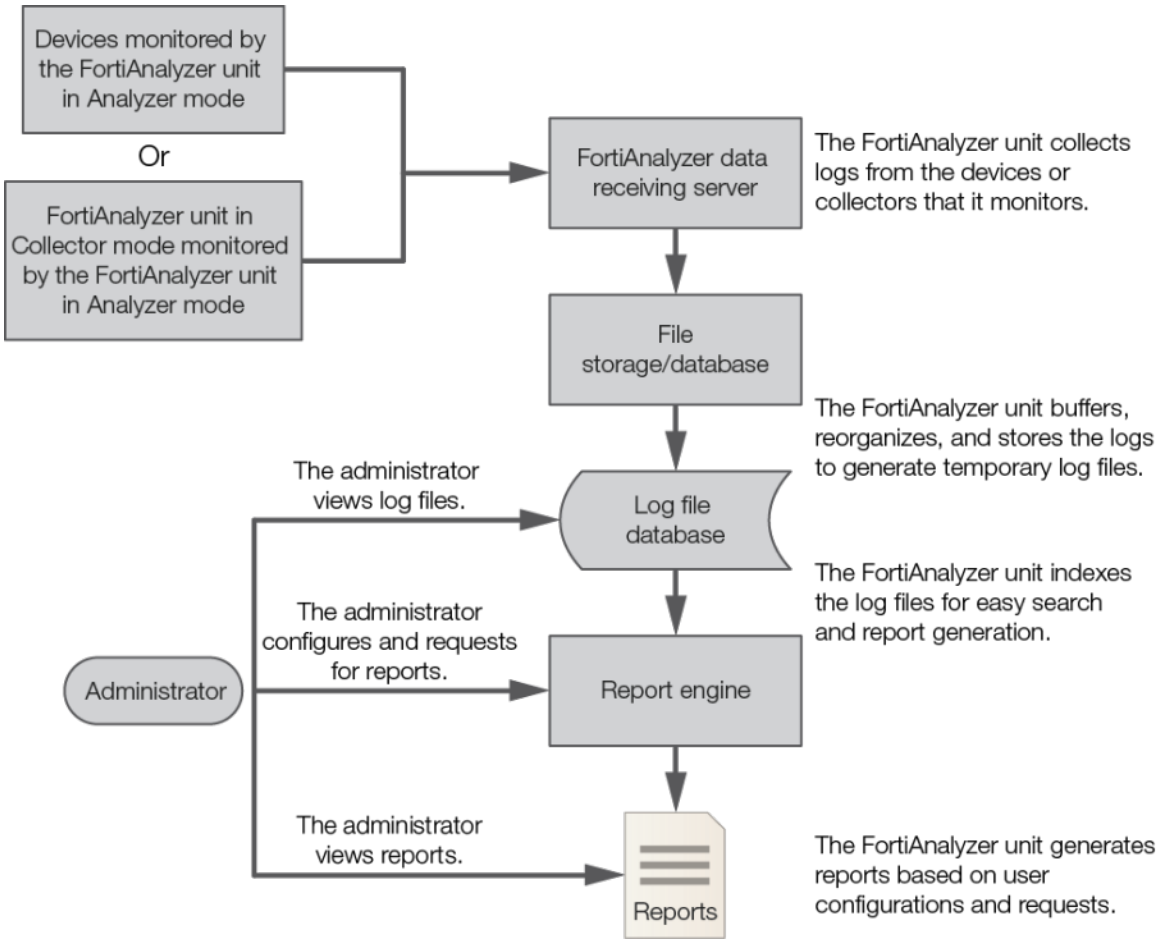
For more information, see Reports on page 156.

Workflow

Once you have successfully deployed the FortiAnalyzer platform in your network, using and maintaining your FortiAnalyzer unit involves the following:

- Configuration of optional features, and re-configuration of required features if required by changes to your network
- Backups
- Updates
- Monitoring reports, logs, and alerts

The following illustration depicts the process of data logging, data analyzing, and report generation by the FortiAnalyzer unit in analyzer mode.


Devices monitored by the FortiAnalyzer unit in Analyzer mode
Or
FortiAnalyzer unit in Collector mode monitored by the FortiAnalyzer unit in Analyzer mode
FortiAnalyzer data receiving server
The FortiAnalyzer unit collects logs from the devices or collectors that it monitors.
File storage/database
The FortiAnalyzer unit buffers, reorganizes, and stores the logs to generate temporary log files.
The administrator views log files.
Log file database
The FortiAnalyzer unit indexes the log files for easy search and report generation.
The administrator configures and requests for reports.
Administrator
Report engine
The administrator views reports.
Reports
The FortiAnalyzer unit generates reports based on user configurations and requests.

GUI

This section describes general information about using the GUI to access the FortiAnalyzer system with a web browser.

This section includes the following topics:

- System requirements
- Connecting to the GUI
- GUI
- GUI configuration
- Reboot and shutdown the FortiAnalyzer unit

Additional configuration options and short-cuts are sometimes available through right-click menus. Right-clicking the mouse in various locations in the GUI accesses these options.

System requirements

Web browser support

The FortiAnalyzer GUI supports the following web browsers:

- Microsoft Internet Explorer versions 10 and 11
- Mozilla Firefox version 35
- Google Chrome version 39

Other web browsers may function correctly, but are not supported by Fortinet.

Screen resolution

Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024. This allows for all the objects in the GUI to be properly viewed.

Please refer to the FortiAnalyzer Release Notes for product integration and support information.

Connecting to the GUI

The FortiAnalyzer unit can be configured and managed using the GUI or the CLI. This section will step you through connecting to the unit via the GUI.

For more information on connecting your specific FortiAnalyzer unit, read that device's Quick Start guide.

To connect to the GUI:

1. Connect the unit to a management computer using an Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiAnalyzer unit:
   - IP address: 192.168.1.2
   - Netmask: 255.255.255.0
3. On the management computer, start a supported web browser and browse to `https://192.168.1.99`.
4. Type `admin` in the *User Name* field, leave the *Password* field blank, and select *Login*.
   You should now be able to use the FortiAnalyzer GUI.

If the network interfaces have been configured differently during installation, the URL and/or permitted administrative access protocols (such as HTTPS) may no longer be in their default state.

For information on enabling administrative access protocols and configuring IP addresses, see Network interfaces on page 75.

If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see Static routes on page 76.

GUI overview

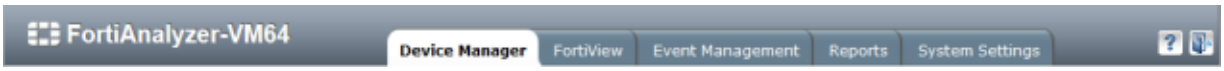
The FortiAnalyzer GUI consists of four primary parts: the tab bar, the main menu bar, the tree menu, and the content pane. The content pane includes a toolbar and, in some tabs, is horizontally split into two sections. The main menu bar is only visible in certain tabs when ADOMs are disabled (see System Information widget on page 53).

You can use the GUI menus, lists, and configuration pages to configure most FortiAnalyzer settings. Configuration changes made using the GUI take effect immediately without resetting the FortiAnalyzer system or interrupting service.

The GUI also includes online help, accessed by selecting the help icon in the right side of the tab bar.

Tab bar

The GUI tab bar contains the device model, the available tabs, the *Help* button and the *Log Out* button.



Device Manager	Manage groups, devices, and VDOMs, and view real-time monitor data. See Device Manager on page 39.

FortiView	Drill down top sources, top applications, top destinations, top web sites, top threats, and top cloud applications. The *Log View* tab is found in the *FortiView* tab. View logs for managed devices. You can display, download, import, and delete logs on this page. You can also define Custom Views.See FortiView on page 114.
Event Management	Configure and view events for managed log devices.See Event Management on page 144. This tab is not available when the unit is in Collector mode. See Operation modes on page 22 for more information.
Reports	Configure report templates, schedules, and output profiles, and manage charts and datasets. See Reports on page 156. This tab is not available when the unit is in Collector mode. See Operation modes on page 22 for more information.
System Settings	Configure system settings, such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See System Settings on page 50.
Change Password	Select to change the password. *Restricted_User* and *Standard_User* admin profiles do not have access to the *System Settings* tab. An administrator with either of these admin profiles will see the change password icon in the navigation pane.
Help	Open the FortiAnalyzer online help.
Log Out	Log out of the GUI.

Tree menu

The GUI tree menu is on the left side of the window. The content in the menu varies depending on which tab is selected and how your FortiAnalyzer unit is configured. If ADOMs are enabled, the contents of the tree menu on all tabs, except the System Settings tab, will be organized by ADOM.

Some elements in the tree menu can be right-clicked to access different configuration options.

Content pane

The content pane is on the right side of the window. The information changes depending on which tab is being viewed and what element is selected in the tree menu. The content pane of the *Device Manager*, *Log View*, and *Reports* tabs is split horizontally into two frames.

GUI configuration

Global settings for the GUI apply regardless of which administrator account you use to log in. Global settings include the idle timeout, TCP port number on which the GUI listens for connection attempts, the network interface(s) on which it listens, and the language of its display.

This section includes the following topics:

- Language support
- Administrative access
- Restricting access by trusted hosts
- Idle timeout

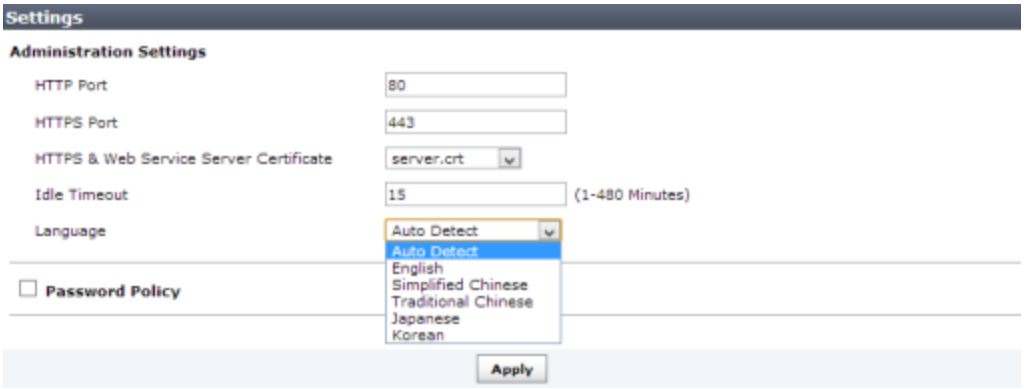
Language support

The GUI supports multiple languages; the default language setting is *Auto Detect*. *Auto Detect* uses the language configured on your management computer. If that language is not supported, the GUI will default to English.

You can change the GUI language to English, Simplified Chinese, Traditional Chinese, Japanese, or Korean. For best results, you should select the language that the management computer operating system uses.

To change the GUI language:

1. Go to *System Settings* > *Admin* > *Admin Settings*.



2. In the *Language* field, select a language from the drop-down list, or select *Auto Detect* to use the same language as configured for your management computer.
3. Select *Apply*.

The following table lists FortiAnalyzer language support information.

Language	GUI	Reports	Documentation
English	✔	✔	✔
Chinese (Simplified)	✔	✔	
Chinese (Traditional)	✔	✔	
French		✔	
Hebrew		✔	
Hungarian		✔	

Language	GUI	Reports	Documentation
Japanese	✔	✔	
Korean	✔	✔	
Portuguese		✔	
Russian		✔	
Spanish		✔	

To change the FortiAnalyzer language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these via the CLI using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the FortiAnalyzer CLI Reference.

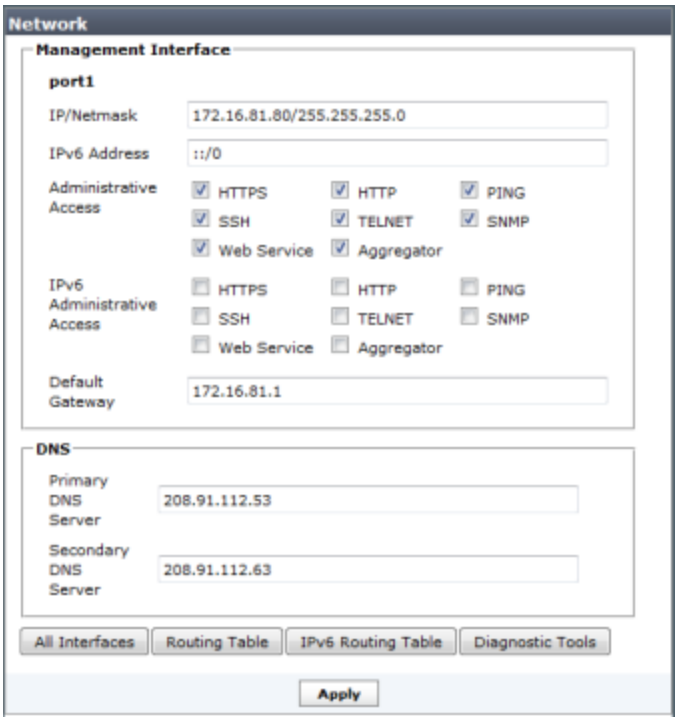
Administrative access

Administrative access enables an administrator to connect to the system to view and change configuration settings. The default configuration of your system allows administrative access to one or more of the interfaces of the unit as described in the QuickStart and installation guides for your device.

Administrative access can be configured in IPv4 or IPv6 and includes settings for: HTTPS, HTTP, PING, SSH (Secure Shell), TELNET, SNMP, Web Service, and Aggregator.

To change administrative access:

1. Go to *System Settings* > *Network*.
   By default, port1 settings will be presented. To configure administrative access for a different interface, select *All Interfaces*, and then select the interface from the list.
2. Set the IPv4 *IP/Netmask* or the *IPv6 Address*, select one or more *Administrative Access* types for the interface, and set the default gateway and Domain Name System (DNS) servers.



3. Select *Apply* to finish changing the access settings.
   For more information, see Network on page 74.

Restricting access by trusted hosts

To prevent unauthorized access to the GUI you can configure administrator accounts with trusted hosts. With trusted hosts configured, the admin user can only log in to the GUI when working on a computer with the trusted host as defined in the admin account. For more information, see Administrator on page 79.

Idle timeout

By default, the GUI disconnects administrative sessions if no activity takes place for fifteen minutes. This idle timeout is recommended to prevent someone from using the GUI from a PC that is logged in and then left unattended.

To change the GUI idle timeout:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Change the *Idle Timeout* minutes as required.
3. Select *Apply* to save the setting.
   For more information, see Administrator settings on page 89.

Reboot and shutdown the FortiAnalyzer unit

Always reboot and shutdown the FortiAnalyzer system using the unit operation options in the GUI or the CLI to avoid potential configuration problems.

To reboot the FortiAnalyzer unit:

1. In the GUI, go to *System Settings* > *Dashboard*.
2. In the *Unit Operation* widget, select *Reboot* or, in the *CLI Console* widget, enter:

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

3. Type `y` to continue. The FortiAnalyzer system will be rebooted.

To shutdown the FortiAnalyzer unit:

1. In the GUI, go to System *Settings* > *Dashboard*.
2. In the *Unit Operation* widget, select *Shutdown* or, in the *CLI Console* widget, enter:

```
execute shutdown
The system will be halted.
Do you want to continue? (y/n)
```

3. Type `y` to continue. The FortiAnalyzer system will be shut down.

To reset the FortiAnalyzer unit:

1. In the *CLI Console* widget, enter:

```
execute reset all-settings
This operation will reset all settings to factory defaults
Do you want to continue? (y/n)
```

2. Type `y` to continue. The device will reset to factory default settings and reboot.

To reset logs and re-transfer all logs into the database:

1. In the *CLI Console* widget, enter:

```
execute reset-sqllog-transfer
WARNING: This operation will re-transfer all logs into database.
Do you want to continue? (y/n)
```

2. Type `y` to continue.

Administrative Domains

When ADOMs are enabled, the *Device Manager* tab has collapsible ADOM navigation, where all of the ADOMs are displayed in the tree menu on the left of the interface. The devices within each ADOM are shown in the default *All FortiGate* group. When ADOMs are disabled, the tree menu simply displays *All FortiGates* and *Unregistered Devices*, if there are any. Non-FortiGate devices are grouped into their own specific ADOMs.

ADOMs are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator. The maximum number of ADOMs you can add depends on the specific FortiAnalyzer system model. Please refer to the FortiAnalyzer data sheet for information on the maximum number of devices and ADOMs that your model supports.

The number of devices within each group is shown in parentheses next to the group name.

ADOMs must be enabled to support non-FortiGate logging and reporting. When a non-FortiGate device is promoted to the DVM table, the device is added to their respective default ADOM and will be visible in the left tree menu. See Adding an ADOM on page 35.

FortiGate and FortiCarrier devices cannot be grouped into the same ADOM. FortiCarrier devices are added to a specific default FortiCarrier ADOM.

To enable the ADOM feature:

1. Log in as `admin`.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, select *Enable* next to *Administrative Domain*.
4. Select *OK* in the confirmation dialog box to enable ADOMs.

To disable the ADOM feature:

1. Remove all log devices from all non-root ADOMs.
2. Delete all non-root ADOMs, by right-clicking on the ADOM in the tree menu in the *Device Manager* tab and selecting *Delete* from the pop-up menu.
3. Go to *System Settings* > *Dashboard*.
4. In the system information widget, select *Disable* next to *Administrative Domain*.
5. Select *OK* in the confirmation dialog box to disable ADOMs.

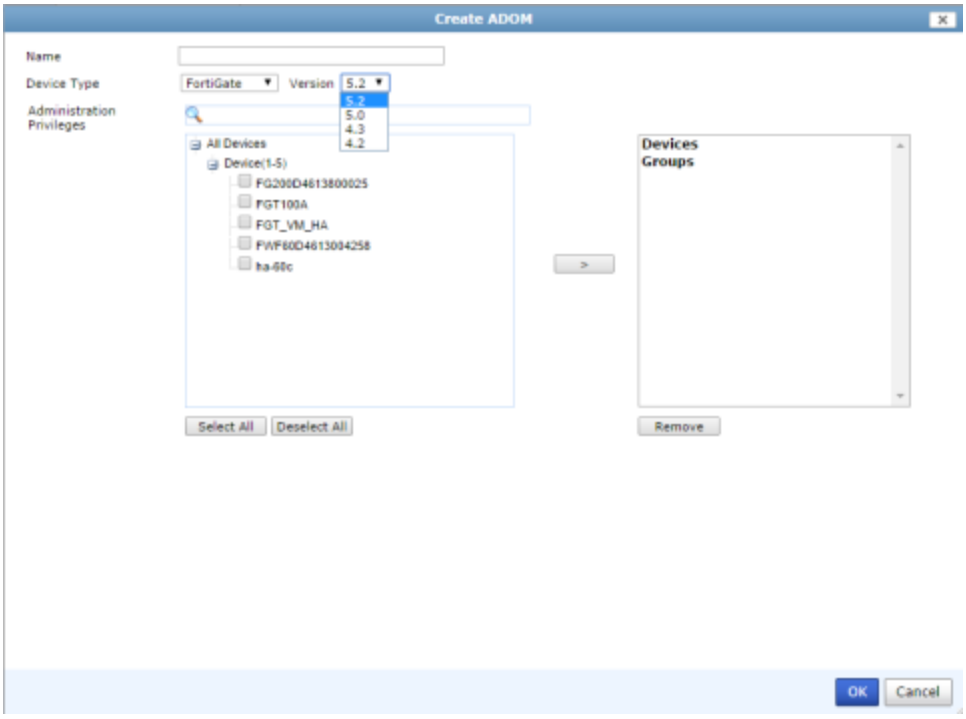
Adding an ADOM

You can create both FortiGate and FortiCarrier ADOMs for versions 5.0, 4.0 MR3, and 4.0 MR2. FortiAnalyzer has default ADOMs for all non-FortiGate devices. When one of these devices is promoted to the DVM table, the device is added to their respective default ADOM and will be visible in the tree menu.

To create a new ADOM:

1. In the *Device Manager* tab, right-click on an ADOM name and, under the ADOM heading, select *Create New*. Alternatively, go to *System Settings* > *All ADOMs* and select *Create New* in the toolbar.

   The *Create ADOM* dialog box opens.



2. Enter the following information:

Name	Enter an unique name that will allow you to distinguish this ADOM from your other ADOMs.
Device Type	Select the device type from the drop-down list. Select one of the following options: FortiGate, FortiCarrier, FortiMail, FortiSandbox, FortiWeb, FortiCache.
Version	Select the firmware version of the devices that will be in the ADOM. The available options is dependent on the device type selected.
Search	Enter a search term to find a specific device (optional).
Devices **Groups**	Transfer devices, VDOMs, and groups from the available member list on the left to the selected member list on the right to assign those devices to the ADOM.

3. Select *OK* to create the ADOM.

To edit an ADOM:

1. In the *Device Manager* tab, right-click on the ADOM you need to edit, then, under the ADOM heading, select *Edit*.
   Alternatively, go to *System Settings* > *All ADOMs*, right-click on the ADOM you need to edit, then select *Edit* in the right-click menu.

   The *Edit ADOM* dialog box opens.
2. Edit the information as required, then select *OK* to apply the changes.

To delete an ADOM:

1. In the *Device Manager* tab, right-click on the ADOM you need to delete, and, under the ADOM heading, select *Delete*.
   Alternatively, go to *System Settings* > *All ADOMs*, right-click on the ADOM you need to delete, and select *Delete* in the right-click menu.

The root ADOM and ADOMs which contains user(s) or device(s) cannot be deleted.

2. Select *OK* in the confirmation dialog box to delete the ADOM.

Assigning devices to an ADOM

The `admin` administrator selects the devices to be included in an ADOM. You cannot assign the same device to two different ADOMs.

To assign devices to an ADOM:

1. On the *Device Manager* tab, in the tree menu, right-click on the ADOM to which you want to assign a device and, under the ADOM heading in the pop-up menu, select *Edit*.
   Alternatively, go to *System Settings* > *All ADOMs*, right-click on the ADOM to which you want to assign a device and, and select *Edit* in the right-click menu

   The *Edit ADOM* dialog box will open.
2. From the *Available member* list, select which devices you want to associate with the ADOM and select the right arrow to move them to the *Selected member* list.
   If the administrative device mode is *Advanced*, you can add separate FortiGate VDOMs to the ADOM as well as FortiGate units.
3. When done, select *OK*. The selected devices appear in the device list for that ADOM.

You can move multiple devices at once. To select multiple devices, select the first device, then hold the Shift key while selecting the last device in a continuous range, or hold the control key while selecting each additional device.

Assigning administrators to an ADOM

The admin administrator can create other administrators and assign an ADOM to their account, constraining them to configurations and data that apply only to devices in their ADOM.

By default, when ADOMs are enabled, existing administrator accounts other than admin are assigned to the root domain, which contains all devices in the device list. For more information about creating other ADOMs, see Adding an ADOM on page 35.

To assign an administrator to an ADOM:

1. Log in as admin.
   Other administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings* > *Admin* > *Administrator*.
3. Configure the administrator account, and select the *Admin Domains* that the administrator account will be able to use to access the FortiAnalyzer system.

Do not select *Edit* for the admin account. The admin administrator account cannot be restricted to an ADOM.

4. Select *OK* to save the setting.
   See Administrator on page 79 for more information.

ADOM device modes

An ADOM has two device modes: normal and advanced. In normal mode, you cannot assign different FortiGate VDOMs to multiple FortiManager ADOMs. The FortiGate unit can only be added to a single ADOM.

In advanced mode, you can assign different VDOMs from the same FortiGate unit to multiple ADOMs.

Advanced ADOM mode will allow users to assign VDOMs from a single device to different ADOMs, but will result in a reduced operation mode and more complicated management scenarios. It is recommended for advanced users only.

To change the ADOM mode, go to *System Settings* > *Advanced* > *Advanced Settings* and change the selection in the *ADOM Mode* field.

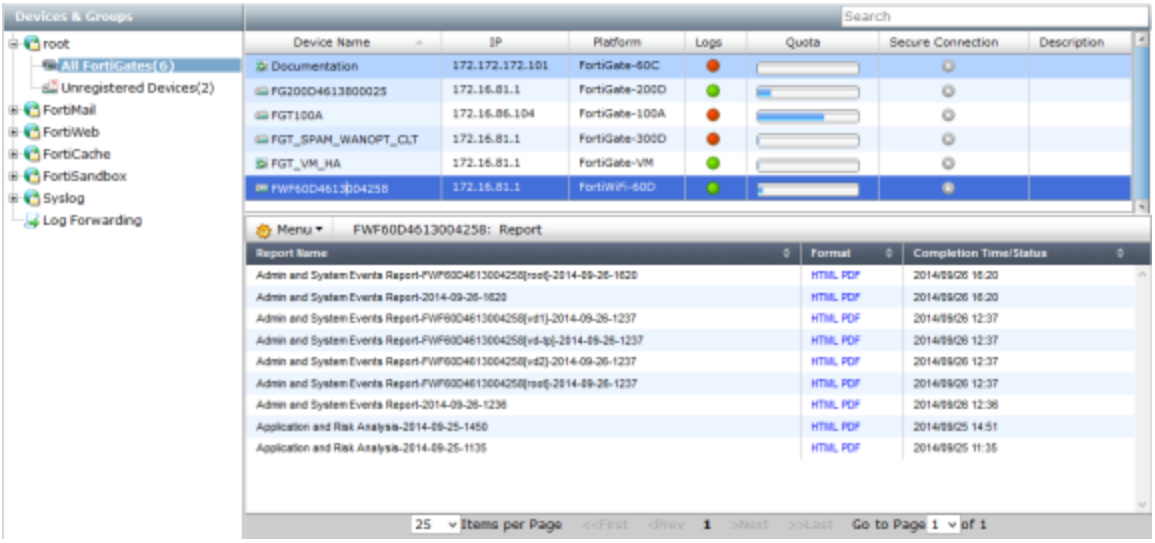
Alternatively, use the following command in the CLI:

```
config system global
   set adom-mode {normal | advanced}
end
```

Normal mode is the default setting. To change from advanced back to normal, you must ensure no FortiGate VDOMs are assigned to an ADOM.

Device Manager

The *Device Manager* tab allows you to add and edit devices and VDOMs, and view completed reports for devices and VDOMs. It also allows you to create, edit, and delete ADOMs when they are enabled.



The tree menu shows the ADOMs and the device within those ADOMs. If ADOMs are disabled, the tree menu simply shows the devices.

The device and VDOM list can be searched using the search box in the content pane toolbar. The columns shown in the list can be customized, and the list can be sorted by selecting a column header.

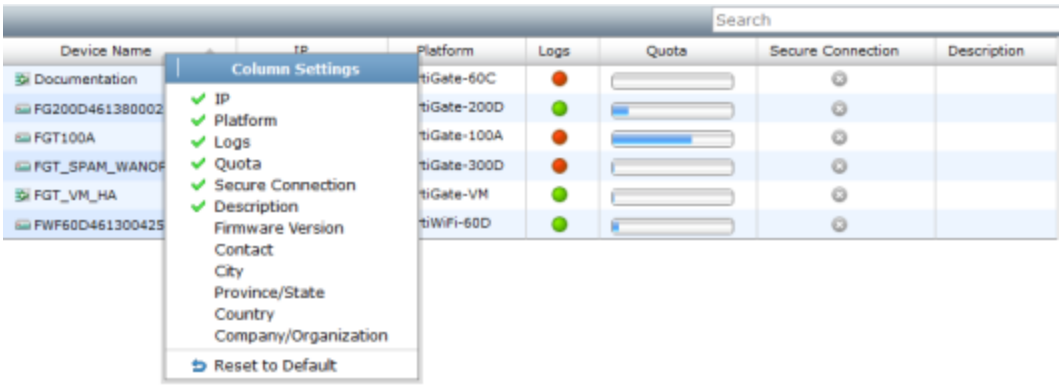
The following column information is available:

Device Name	The device name. The icon displayed to the left of the device name indicates if the device is standalone or part of a high availability cluster. Cluster members are not displayed in this screen. You can view and edit cluster member when selecting to edit the device.
IP	The device IP address.
Platform	The device platform type, for example, FortiGate-60C.
Logs	The icon displayed indicates if logging is enabled. Hover over the icon for additional information.
Quota	The percent of disk log quota used is displayed. Hover over the bar to see the exact percentage. You can view and edit the disk log quota when selecting to edit the device.
Secure Connection	The icon displayed indicates if secure connection is enabled. Hover over the icon to view the IPsec VPN tunnel status.

Description	Displays the user defined description. You can view and edit the device description when selecting to edit the device.
Firmware Version	The firmware version.
Contact	Displays the user defined contact. You can view and edit this field when selecting to edit the device.
City	Displays the user defined city. You can view and edit this field when selecting to edit the device.
Province/State	Displays the user defined province/state. You can view and edit this field when selecting to edit the device.
Country	Displays the user defined country. You can view and edit this field when selecting to edit the device.
Company/Organization	Displays the user defined company/organization. You can view and edit this field when selecting to edit the device.

To change the column settings:

1. Right-click on a column heading in the content pane.
   Columns currently included in the content pane table have a green check mark next them.



2. Select a column from the list to add or remove that column from the table, or select *Reset to Default* to reset the table to its default state

Devices

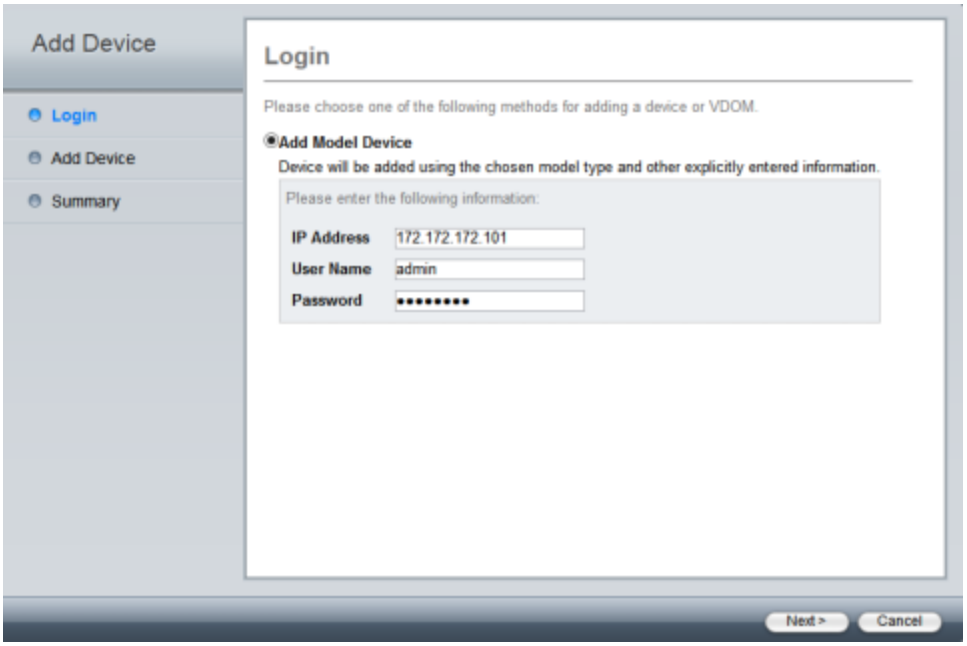
Devices are organized by device type. VDOMs and model devices can be created and deleted.

Devices and VDOMs

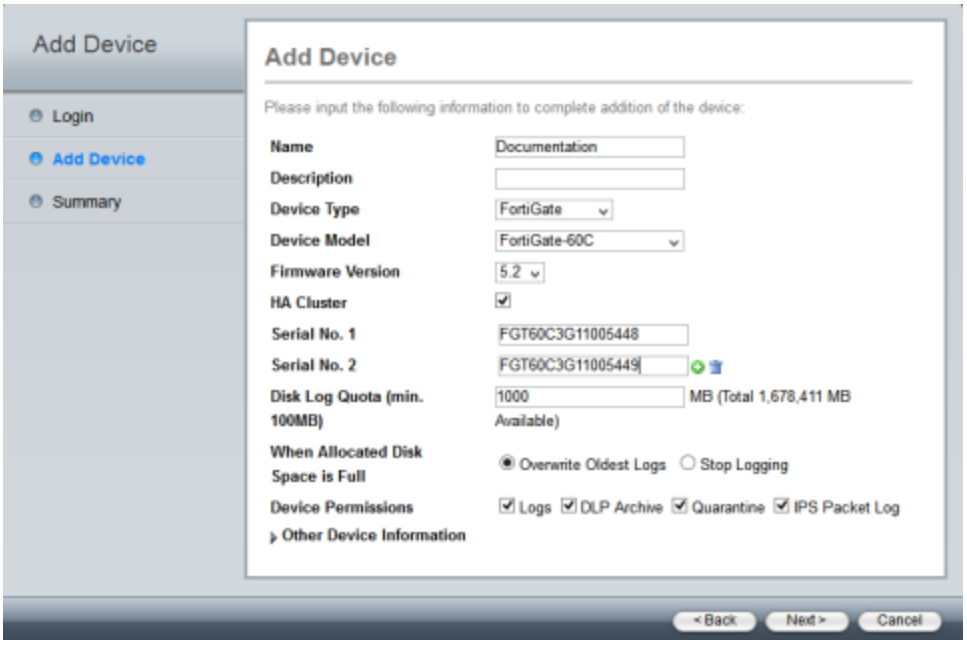
Device models can be added and deleted, devices can be edited, and VDOMs can be deleted. The *Add Device* wizard is used to add model devices.

To add a model device:

1. Right-click on a group in the tree menu or in the content pane and, from the right-click menu, select *Add Device*, or, if ADOMs are not enabled, select *Add Device* from the toolbar. The *Add Device* wizard opens.



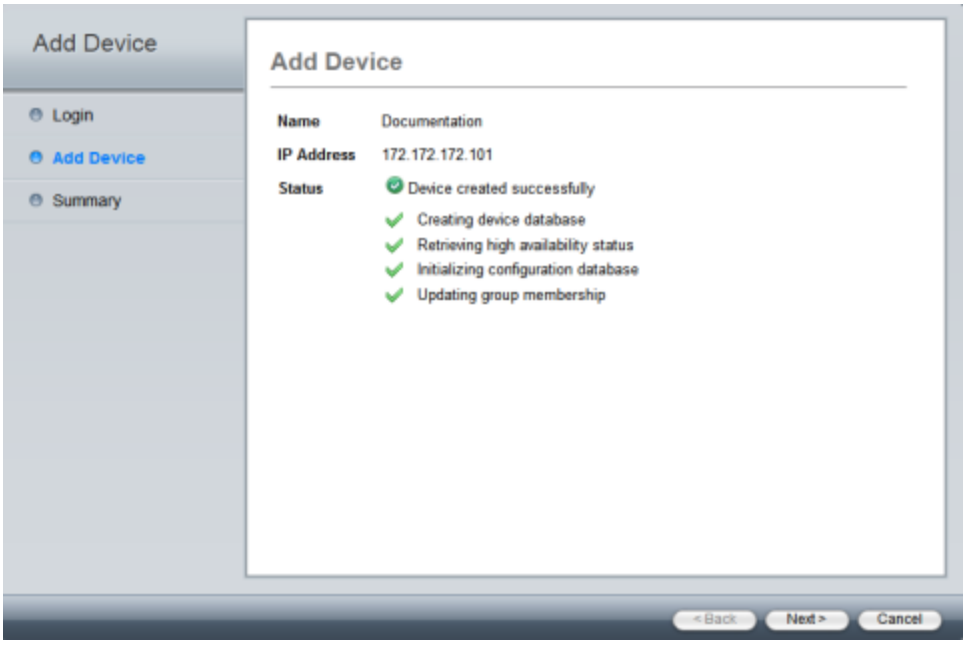
2. Enter the device IP address, user name, and password in the requisite fields.
3. Select *Next* to continue to the next page of the wizard: *Add Device*.



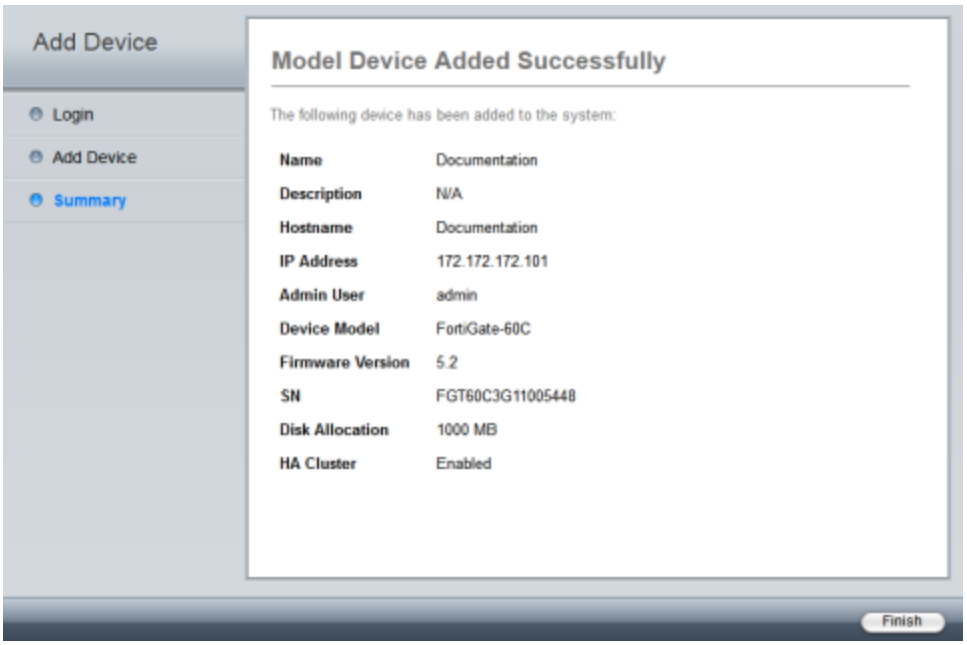
4. Enter the following information:

Name	Enter a name for the device.
Description	Enter a description for the device (optional).
Device Type	Select the device type from the drop-down list. Select FortiGate for FortiGate ADOMs, FortiSwitch for FortiSwitch ADOMs, etc.
Device Model	Select the device model from the drop-down list.
Firmware Version	Select the firmware version from the drop-down list.
HA Cluster	Select if the device is part of a high availability cluster.
Serial Number	Enter the device serial number. This value must match the device model selected. When HA Cluster is enabled, you can enter the serial numbers of all members of the cluster.
Disk Log Quota (min. 100MB)	Enter the disk log quota in MB. This option is only available for certain device types.
When Allocated Disk Space is Full	Select to overwrite the oldest logs or to stop logging when the allocated disk space is full.
Device Permissions	Select the device permissions from: *Logs, DLP Archive, Quarantine*, and *IPS Packet Log*.
Other Device Information	Enter other device information (optional), including: *Company/Organization*, *Contact*, *City*, *Province/State*, and *Country*.

5. Select *Next* to proceed to the next add device page.



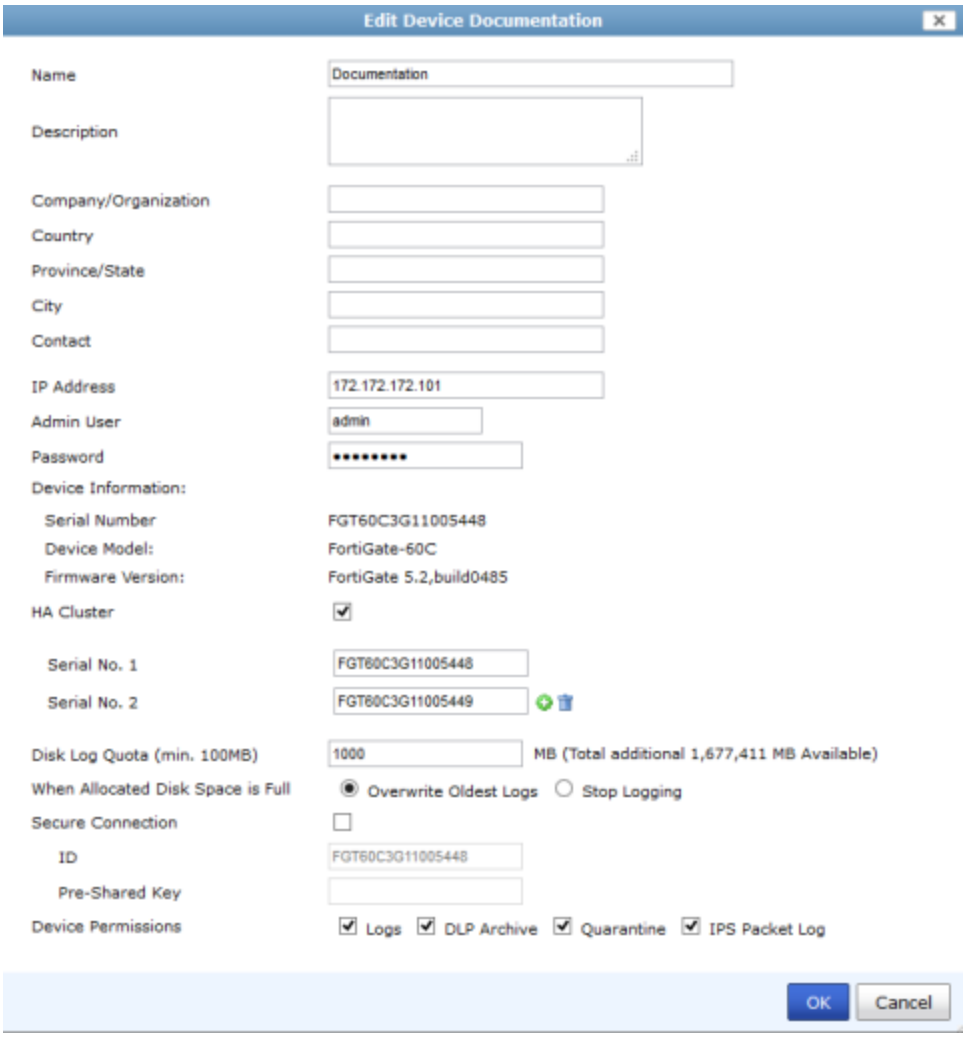
6. After the device has been created successfully, select *Next* to proceed to the summary page.



7. Select *Finish* to add the device model.

To edit a device:

1. In the *Device Manager* tab, in the tree menu, select the group that contains the device you need to edit.
2. In the content pane, right-click on the on the device and select *Edit* from the right-click menu.
   The *Edit Device* dialog box opens.



3. Edit the following information as needed:

Name	The name of the device.
Description	Descriptive information about the device.
Company/Organization	Company or organization information.
Country	Enter the country.
Province/State	Enter the province or state.
City	Enter the city.
Contact	Enter the contact name.
IP Address	The IP address of the device.
Admin User	The administrator username.

Password	The administrator password.
Device Information	Information about the device, including serial number, device model, firmware version, connected interface.
HA Cluster	Select if the device is part of a high availability cluster.
Serial No.	When HA Cluster is enabled, you can enter the serial numbers of all members of the cluster.
Disk Log Quota (min. 100MB)	The amount of space that the disk log is allowed to use, in MB.
When Allocated Disk Space is Full	The action for the system to take when the disk log quota is filled, either *Overwrite Oldest Logs*, or *Stop Logging*.
Secure Connection	Select check box to enable this feature. Secure Connection secures Odette File Transfer Protocol (OFTP) traffic through an IPsec tunnel.
ID	The device serial number.
Pre-Shared Key	The pre-shared key for the IPsec connection between the FortiGate and FortiAnalyzer.
Device Permissions	The device's permissions. Select any of: *Logs*, *DLP Archive*, *Quarantine*, and *IPS Packet Log*.

4. Select *OK* to finish editing the device.

To delete a device or VDOM:

1. In the *Device Manager* tab, in the tree menu, select the group that contains the device or VDOM you need to delete.
2. In the content pane, right-click on the on the device or VDOM and select *Delete* in the right-click menu.
3. Select *OK* in the confirmation window to delete the device or VDOM.

FortiGate HA clusters

FortiAnalyzer v5.0.8 and later supports FortiGate HA clusters for device registration, event management, logging, and reports.

When creating a FortiGate HA cluster, a device CID is created for the cluster. Although the cluster members are not visible in the Device Manager, you can view and edit cluster settings when selecting to edit the device. To view the additional HA cluster information, enter the `diagnose log device` command in the CLI console.

Example output:

```
Documentation   FGHA000404997363_CID   0MB(0 / 0 / 0 / 0 / 0 )   1000MB   0.00%
   |- HA cluster member: FGT60C3G11005448
   |- HA cluster member: FGT60C3G11005449
```

To add an HA cluster using the Add Device Wizard:

1. In the Device Manager tab, right-click on the ADOM and select *Add Device* from the menu.
   The *Add Device* wizard is displayed.

2. Enter the IP address, user name, and password of the primary device.
3. Select *Next* to continue.
4. Enter the applicable information. The disk log quota entered is for the HA cluster.
5. Select to enable *HA Cluster* and enter the serial numbers of all cluster member devices.
6. Select *Next* to create the device cluster, select *Next* to view the summary, and select *Finish* to complete the wizard.
7. Once the FortiGate is configured to send logs to FortiAnalyzer, all HA cluster logs (master and slave) are stored in the directory `/Storage/Logs/FGHA00xxxxxxxx_CID`.

To promote an HA cluster:

1. Configure the FortiGate to send logs to FortiAnalyzer.
2. On the FortiAnalyzer, the HA cluster will be listed in the unregistered device table. All members of the HA cluster will be visible in this table.

The unregistered device pop-up dialog box does not reference the HA status. This information is only available in the *Unregistered Devices* tree menu.

3. Promote the HA cluster. The HA cluster in registered in Device Manager and a FGHA CID is created.
4. Once the FortiGate is configured to send logs to FortiAnalyzer, all HA cluster logs (master and slave) are stored in the directory `/Storage/Logs/FGHA00xxxxxxxx_CID`.

To edit existing devices and enable an HA cluster while ignoring old log data:

1. In the Device Manager tab, edit the FortiGate device, enable HA Cluster, and add the cluster serial numbers.
2. The HA cluster is registered in Device Manager and a FGHA CID is created.
3. Remove the HA cluster members from Device Manager.
4. All existing log data will be removed and all HA cluster logs (master and slave) are stored in the directory `/Storage/Logs/FGHA00xxxxxxxx_CID`.

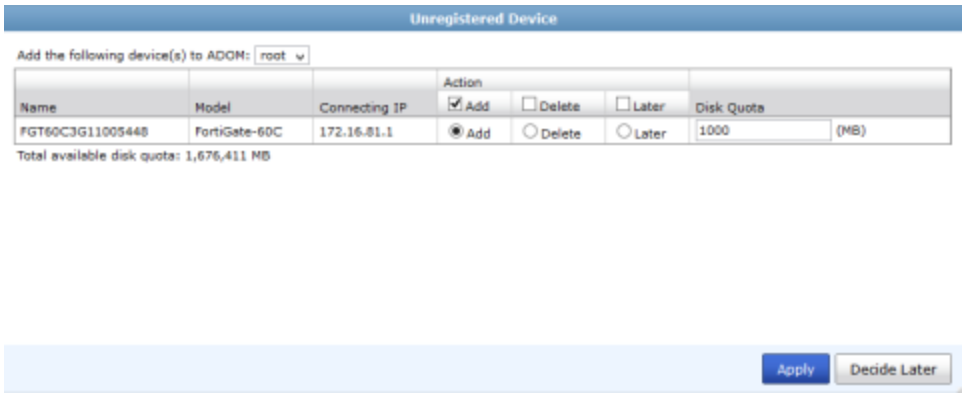
To edit existing devices and enable an HA cluster while keeping old log data:

1. In the Device Manager tab, edit the FortiGate device, enable HA Cluster, and add the cluster serial numbers.
2. The HA cluster is registered in Device Manager and a FGHA CID is created.
3. Check for zombie device. To view the all log devices, enter the `execute log device logstore list` command in the CLI console.
4. Move log files from zombie devices to the FGHA CID device. To move log files use the following CLI command:
   ```
   execute log device logstore move <zombie_device_ID> <FGHA_CID_device_ID>
   ```
   Enter `y` to continue. Log files in the zombie devices are removed.
5. Remove the HA cluster members from Device Manager.
6. Clear zombie directories using the following CLI command:
   ```
   execute log device logstore clear All
   ```
   Enter `y` to continue. This will remove all zombie device logs and archive files.
7. Rebuild the SQL database using the following CLI command:
   ```
   execute sql-local rebuild-db
   ```
   Enter `y` to continue. The existing SQL database will be removed and rebuilt from log data.

The `execute sql-local rebuild-db` command requires a reboot to complete. The time required to rebuild the SQL database is dependent on the amount of log data.

Unregistered devices

In FortiAnalyzer v5.0.4 and later, the `config system global > set unregister-pop-up` command is enabled by default. When a device is configured to send logs to FortiAnalyzer, the unregistered device table will be displayed. You can decide to add devices to specific ADOMs now, at a later date, or to delete the device.



In FortiAnalyzer v5.0.5 or later, the `config system global > set unregister-pop-up` command is disabled by default. When a device is configured to send logs to FortiAnalyzer, the unregistered device table will not be displayed. Instead, a new entry *Unregistered Devices* will appear in the Device Manager tab tree menu. You can then promote devices to specific ADOMs or use the right-click menu to delete the device.

Device reports

You can view, download, and delete device reports in the *Device Manager* content pane. Selecting a device or VDOM in the tree menu will display all reports associated with that device or VDOM in the content pane. For more information, see View report tab on page 163.

To view latest reports from the Device Manager tab:

1. In the *Device Manager* tab select the ADOM that contains the device whose reports you would like to view.
2. Select the device or VDOM from the tree menu.
3. The report history is shown in the lower content pane, showing a list of all the reports that have been run for that device or VDOM.
4. Click on a report to display the report in a browser window or download it to your management computer.

Log forwarding

You can configure log forwarding in the Device Manager tab. You can configure to forward logs for selected devices to another FortiAnalyzer, a syslog server, or a Common Event Format (CEF) server.

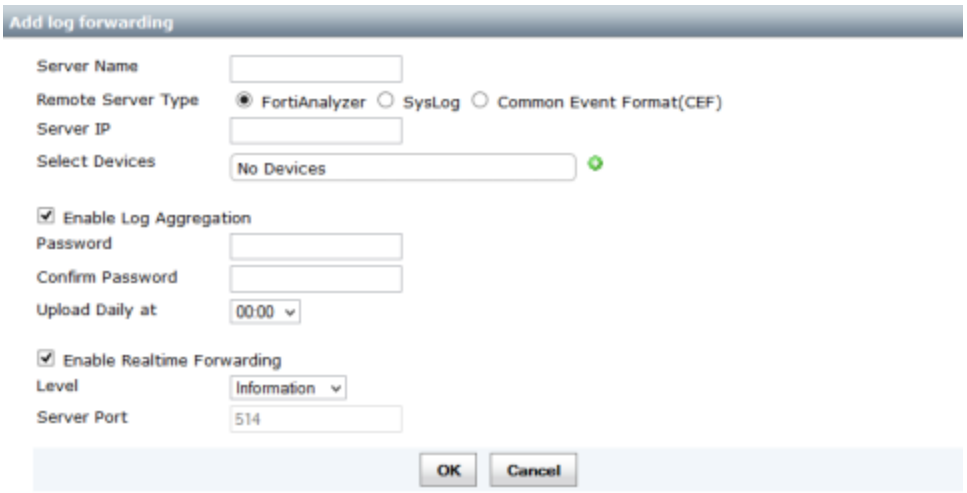
To enable log forwarding:

1. Go to *System Settings* > *Dashboard*.
2. In the *CLI Console* widget enter the following CLI commands:

```
config system admin setting
   set show-log-forwarding enable
end
```

To configure log forwarding:

1. Go to the *Device Manager* tab and select *Log Forwarding*.
2. Select *Create New* from the toolbar.
   The *Add log forwarding* page is displayed.



3. Configure the following settings:

Server Name	Enter a name to identify the remote server.
Remote Server Type	Select the remote server type. Select one of the following: *FortiAnalyzer*, *Syslog*, *Common Event Format (CEF)*.
Server IP	Enter the server IP address.
Select Devices	Select the add icon to select devices. Select devices and select *OK* to add the devices.
Enable Log Aggregation	Select to enable log aggregation. This option is only available when *Remote Server Type* is set to *FortiAnalyzer*.
Password	Enter the server password.
Confirm Password	Re-enter the server password.
Upload Daily at	Select a time from the drop-down list.

Enable Real-time Forwarding	Select to enable real-time log forwarding.
Level	Select the logging level from the drop-down list. Select one of the following: *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notification*, *Information*, or *Debug*.
Server Port	Enter the server port. When *Remote Server Type* is *FortiAnalyzer*, the port cannot be changed. The default port is 514.

4. Select *OK* to save the setting.

Disk space allocation

In FortiAnalyzer, the system reserves 5% to 25% disk space for system usage and unexpected quota overflow. Only 75% to 95% disk space is available for allocation to devices.

Disk Size	Reserved Disk Quota
Small Disk(less than 500GB)	The system reserves either 20% or 50GB of disk space, whichever is smaller.
Medium Disk(less than 1000GB)	The system reserves either 15% or 100GB of disk space, whichever is smaller.
Large Disk(less than 3000GB)	The system reserves either 10% or 200GB of disk space, whichever is smaller.
Very Large Disk(less than 5000GB)	The system reserves either 5% or 500GB of disk space, whichever is smaller.
Note: The RAID level selected will impact the determination of the disk dize and reserved disk quota level. For example, a FAZ-1000C with four 1TB hard drives configured in RAID 10 will be considered a large disk and 10% or 200GB disk space will be reserved.	

Log arrays in FortiAnalyzer v5.0.7 and later

The concept of log array changed between FortiAnalyzer v5.0.6 and FortiAnalyzer v5.0.7.

In FortiAnalyzer v5.0.6 and earlier, log arrays can be treated as a single device which has its own SQL database. The size of its database is enforced by the log array quota.

In FortiAnalyzer v5.0.7 and later, log array is only a grouping concept which is used to display logs or generate reports for a group of devices. It has no SQL database and does not occupy additional disk space.

System Settings

The *System Settings* tab enables you to manage and configure system options for the FortiAnalyzer unit. This includes the basic network settings to connect the device to the corporate network, the configuration of administrators and their access privileges, and managing and updating firmware for the device.

Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the GUI page to access these options.

The *System Settings* tab provides access to the following menus and sub-menus:

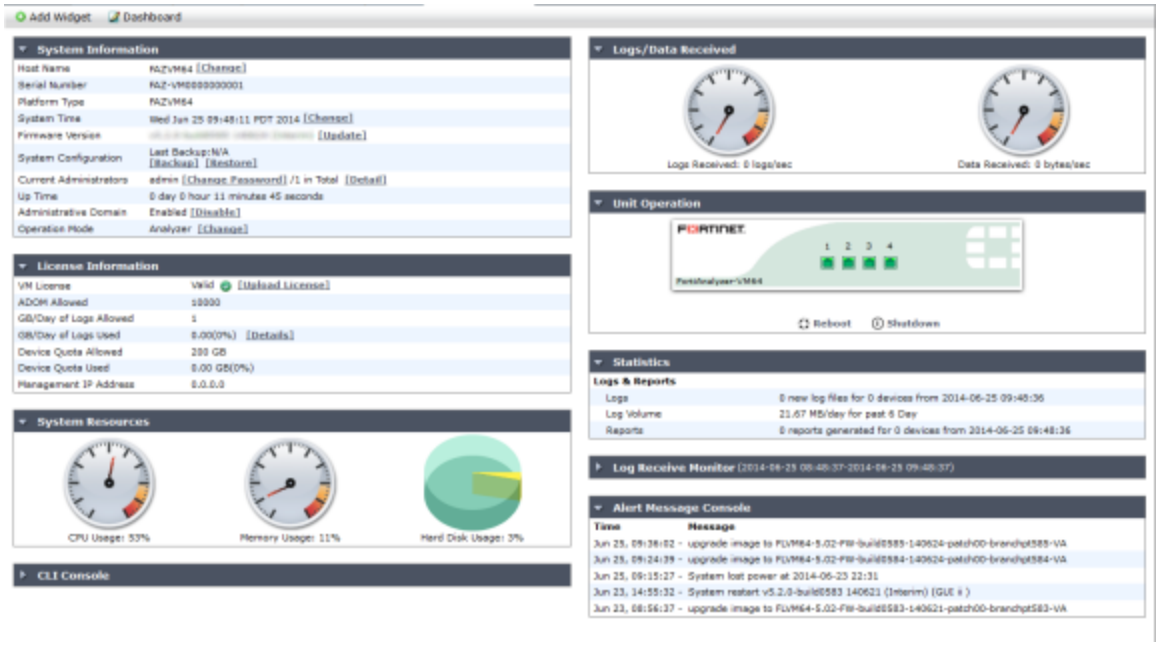
Dashboard	Select this menu to configure, monitor, and troubleshoot your FortiAnalyzer device. Dashboard widgets include: System Information, License Information, Unit Operation, System Resources, Alert Message Console, CLI Console, Log Receive Monitor, Logs/Data Received, Statistics, Insert Rate vs Receive Rate, and Log Insert Lag Time.
All ADOMs	Select this menu to create new ADOMs and monitor all existing ADOMs.
RAID management	Select this menu to configure and monitor your Redundant Array of Independent Disks (RAID) setup. This page displays information about the status of RAID disks as well as what RAID level has been selected. It also displays how much disk space is currently consumed.
Network	Select this menu to configure your FortiAnalyzer interfaces. You can also view the IPv4/IPv6 Routing Table and access Diagnostic Tools.
Admin	Select this menu to configure administrator user accounts, as well as configure global administrative settings for the FortiAnalyzer unit. • Administrator • Profile • Remote authentication server • Administrator settings
Certificates	Select this menu to configure the following: • Local certificates • CA certificates • Certificate revocation lists
Event log	Select this menu to view FortiAnalyzer event log messages. On this page you can: • Download the logs in `.log` or `.csv` formats • View raw logs or logs in a formatted table • Browse the event log, FDS upload log, and FDS download log

Task monitor	Select this menu to monitor FortiAnalyzer tasks.
Advanced	Select to configure advanced settings. • SNMP v1/v2c • Mail server • Syslog server • Meta fields • Device log settings • File management • Advanced settings

Dashboard

When you select the *System Settings* tab, it automatically opens at the *System Settings* > *Dashboard* page.

The *Dashboard* page displays widgets that provide performance and status information and enable you to configure basic system settings. The dashboard also contains a CLI widget that enables you to use the command line through the GUI. These widgets appear on a single dashboard.



The following widgets are available:

System Information	Displays and allow editing of some basic information about the FortiAnalyzer system, including host name, serial number, platform type, system time, firmware version, system configuration, current administrators, up time, administrative domains, and operation mode. From this widget you can manually update the FortiAnalyzer firmware to a different release. For more information, see System Information widget on page 53.
License Information	Displays the devices being managed by the FortiAnalyzer unit, the maximum numbers of devices allowed, the maximum number of ADOMs allowed, GB/Day of logs allowed, and GB/Day of logs used. FortiAnalyzer VM also includes device quota allowed, device quota used, and management IP address fields. For more information, see License Information widget on page 58.
Unit Operation	Displays status and connection information for the ports of the FortiAnalyzer unit. It also enables you to shutdown and reboot the FortiAnalyzer unit. For more information, see Unit Operation widget on page 59.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 59.
Alert Message Console	Displays log-based alert messages for both the FortiAnalyzer unit itself and connected devices. For more information, see Alert Messages Console widget on page 61.
CLI Console	Opens a terminal window that enables you to configure the FortiAnalyzer unit using CLI commands directly from the GUI. For more information, see CLI Console widget on page 62.
Log Receive Monitor	Displays a real-time graph of logs received. You can select to view data per device or per log type. For more information, see Log Receive Monitor widget on page 63.
Logs/Data Received	Displays the real-time or historical usage status of logs received and data received. For more information, see Logs/Data Received widget on page 63.
Statistics	Displays statistics for logs and reports since last reset. For more information, see Statistics widget on page 64.
Insert Rate vs Receive Rate	Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 65
Log Insert Lag Time	Displays the log insert lag time, in seconds. For more information, see Log Insert Lag Time widget on page 65

Customizing the dashboard

The FortiAnalyzer system settings dashboard is customizable. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

To move a widget

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To add a widget

In the dashboard toolbar, select *Add Widget*, then select the names of widgets that you want to show. To remove a widget, select the *Close* icon in the widget title bar.

To reset the dashboard

In the dashboard toolbar, select *Dashboard* > *Reset Dashboards*, then select *OK* in the confirmation dialog box. The dashboards will be reset to the default view, which includes everything except the *CLI Console* widget.

To see the available options for a widget

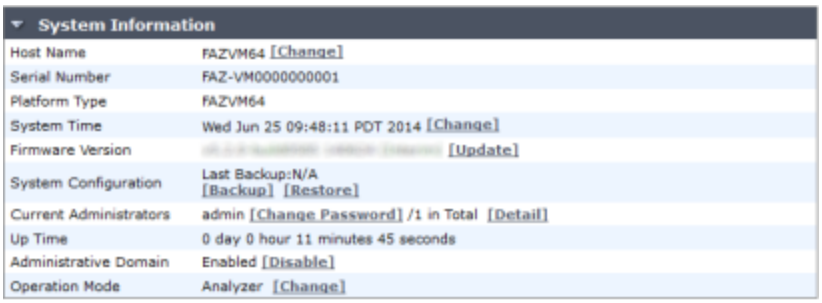
Position your mouse cursor over the widget's title bar. Options vary slightly from widget to widget, but always include options to close or show/hide the widget.

The following table lists the widget options.

Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
More Alerts	Show the *Alert Messages* dialog box. This option appears only in the *Alert Message Console* widget.
Edit	Select to change settings for the widget.This option appears only in certain widgets.
Detach	Detach the *CLI Console* widget from the dashboard and open it in a separate window. This option appears only in the *CLI Console* widget.
Reset	Select to reset the information shown in the widget. This option appears only in the *Statistics* widget.
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action.

System Information widget

The *System Information* widget, shown below, displays the current status of the FortiAnalyzer unit and enables you to configure basic system settings.



The following information is available on this widget:

Host Name	The identifying name assigned to this FortiAnalyzer unit. For more information, see Changing the host name on page 55.
Serial Number	The serial number of the FortiAnalyzer unit. The serial number is unique to the FortiAnalyzer unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	This field is displayed for FortiAnalyzer VM and shows the VM platform type on which the FortiAnalyzer is installed.
System Time	The current date, time, and time zone on the FortiAnalyzer internal clock or Network Time Protocol (NTP) server. For more information, see Setting the date and time on page 55.
Firmware Version	The version number and build number of the firmware installed on the FortiAnalyzer unit. To update the firmware, you must download the latest version from the Customer Service & Support portal at https://support.fortinet.com. Select *Update* and select the firmware image to load from your management computer. For more information, see the FortiAnalyzer Release Notes in the Fortinet Document Library.
System Configuration	The date of the last system configuration backup. The following actions are available: Select *Backup* to backup the system configuration to a file; see Backing up the system on page 56. Select *Restore* to restore the configuration from a backup file; see Restoring the configuration on page 57.
Current Administrators	The number of administrators that are currently logged in. The following actions are available: Select *Change Password* to change your own password. Select *Details* to view the session details for all currently logged in administrators. See Monitoring administrator sessions on page 78 for more information.
Up Time	The duration of time the FortiAnalyzer unit has been running since it was last started or restarted.

Administrative Domain	Displays whether ADOMs are enabled, and allows for enabling and disabling ADOMs. See Administrative Domains on page 35 for more information.
Operation Mode	Display and change the current operating mode. Note that not all models support all operation modes. See Changing the operation mode on page 57.

Changing the host name

The host name of the FortiAnalyzer unit is used in several places.

- It appears in the *System Information* widget on the *Dashboard*. For more information about the *System Information* widget, see System Information widget on page 53.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name. .

The *System Information* widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed.

For example, if the host name is Fortinet1234567890, the CLI prompt would be `Fortinet123456~#`.

To change the host name:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Host Name* field, select *Change*. The *Change Host Name* dialog box opens.
3. In the *Host Name* field, type a new host name.

   The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
4. Select *OK* to save the setting.

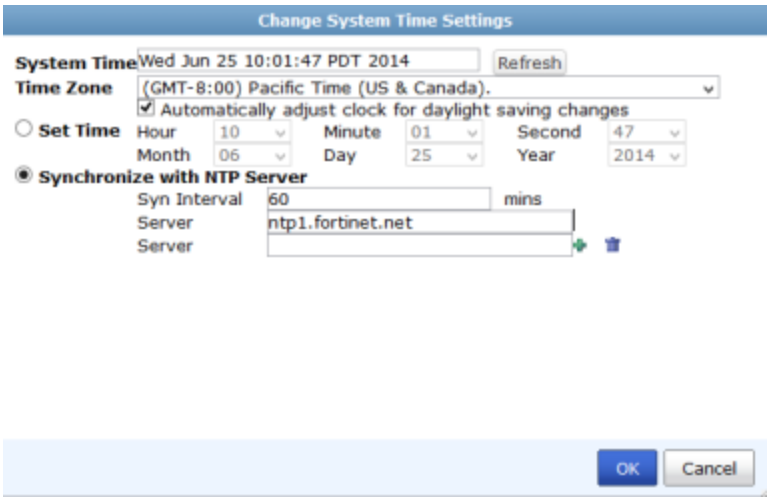
Setting the date and time

You can either manually set the FortiAnalyzer system time and date, or configure the FortiAnalyzer unit to automatically keep its system time correct by synchronizing with an NTP server.

For many features to work, including scheduling, logging, and SSL-dependent features, the FortiAnalyzer system time must be accurate.

To configure the date and time:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *System Time* field, select *Change*. The *Change System Time Settings* dialog box appears.



3. Configure the following settings to either manually set the system time, or to automatically synchronize the FortiAnalyzer unit's clock with an NTP server:

System Time	The date and time according to the FortiAnalyzer unit's clock at the time that this tab was loaded, or when you last selected the *Refresh* button for the *System Information* widget.
Time Zone	Select the time zone in which the FortiAnalyzer unit is located and whether or not the system automatically adjusts for daylight savings time.
Set Time	Select this option to manually set the date and time of the FortiAnalyzer unit's clock, then select the *Hour*, *Minute*, *Second*, *Year*, *Month*, and *Day* fields before you select *OK*.
Synchronize with NTP Server	Select this option to automatically synchronize the date and time of the FortiAnalyzer unit's clock with an NTP server, then configure the *Syn Interval* and *Server* fields before you select *OK*. Select the add icon to add multiple NTP servers. Select the delete icon to remove servers.
Sync Interval	Enter how often in minutes the FortiAnalyzer unit should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.
Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to http://www.ntp.org.

4. Select *OK* to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, the device firmware can be upgraded. For information about a specific firmware version, see the FortiAnalyzer Release Notes in the Fortinet Document Library.

Backing up the system

Fortinet recommends that you back up your FortiAnalyzer configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with

minimal effect to the network. You should also perform a back up after making any changes to the FortiAnalyzer configuration or settings that affect the log devices.

You can perform backups manually. Fortinet recommends backing up all configuration settings from your FortiAnalyzer unit before upgrading the FortiAnalyzer firmware.

To back up the FortiAnalyzer configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *System Configuration* field, select *Backup*. The *Backup* dialog box appears.
3. Configure the following settings:

Encryption	Select to encrypt the backup file with a password. The password is required to restore the configuration. The check box is selected by default.
Password	Select a password. This password is used to encrypt the backup file, and is required to restore the file. (This option is available only when the encryption check box is selected.)
Confirm Password	Re-enter the password to confirm it.

4. If you want to encrypt the backup file, select the *Encryption* check box, then enter and confirm the password you want to use.
5. Select *OK* and save the backup file on your management computer.

Restoring the configuration

You can use the following procedure to restore your FortiAnalyzer configuration from a backup file on your management computer.

To restore the FortiAnalyzer configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *System Configuration* field, select *Restore*. The *Restore* dialog box appears. The *Restore* dialog box appears.
3. Configure the following settings:

From Local	Select *Browse* to find the configuration backup file you want to restore on your management computer.
Password	Enter the encryption password, if applicable.
Overwrite current IP, routing	Select the check box if you need to overwrite the current IP and routing settings.

4. Select *OK* to proceed with the configuration restore.

Changing the operation mode

The FortiAnalyzer unit has two operation modes: analyzer and collector. For more information, see Operation modes on page 22.

Not all FortiAnalyzer models support all operation modes.

To change the operation mode:

1. On the FortiAnalyzer unit, go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Operation Mode* field, select *Change*. The *Change Operation Mode* dialog box opens.
3. Configure the following settings:

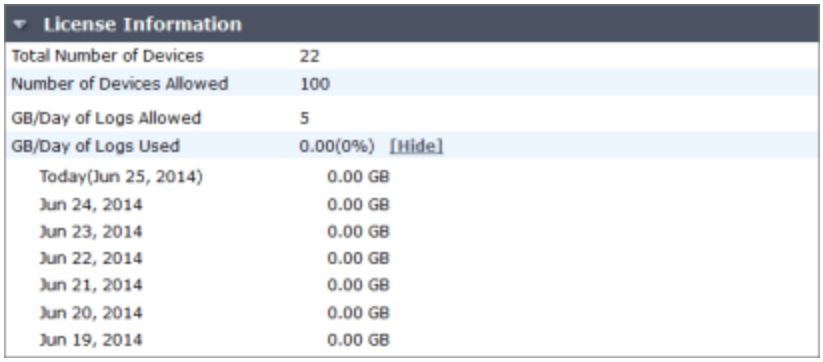
Analyzer	Select to configure FortiAnalyzer in analyzer mode.
Collector	Select to configure FortiAnalyzer in collector mode.

4. Select *OK* to change the operation mode.

License Information widget

The license information displayed on the dashboard shows information on features that vary by a purchased license or contract, such as FortiGuard subscription services. It also displays how many devices are connected or attempting to connect to the FortiAnalyzer unit.

The information displayed in the license information widget will vary between physical and VM FortiAnalyzer units.



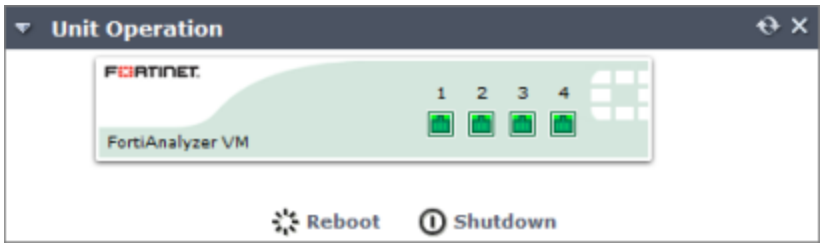
The VM license information widget displays similar information but includes the VM license information and management IP address, as well as the ability to upload a VM license.

To upload a FortiAnalyzer VM license:

1. Go to *System Settings* > *Dashboard*.
2. In the *License Information* widget, in the *VM License* field, select *Upload License*.
3. Browse to the VM license file on your management computer.
4. Select *OK* to load the license file.

Unit Operation widget

The Unit Operation widget is a graphical representation of the FortiAnalyzer unit. It displays status and connection information for the ports on the FortiAnalyzer unit. It also enables you to quickly reboot or shutdown the FortiAnalyzer device.

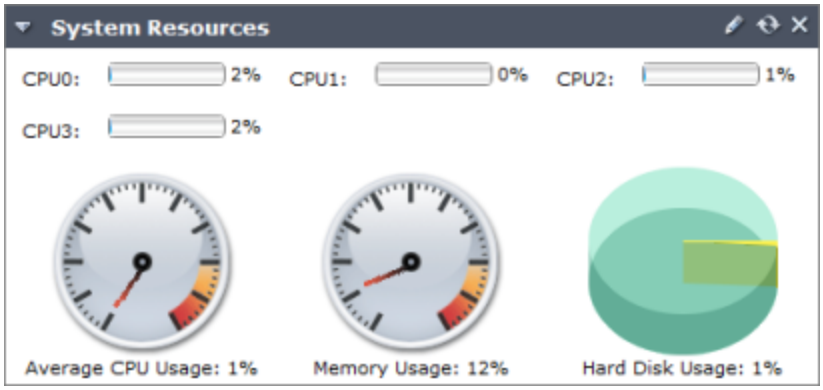


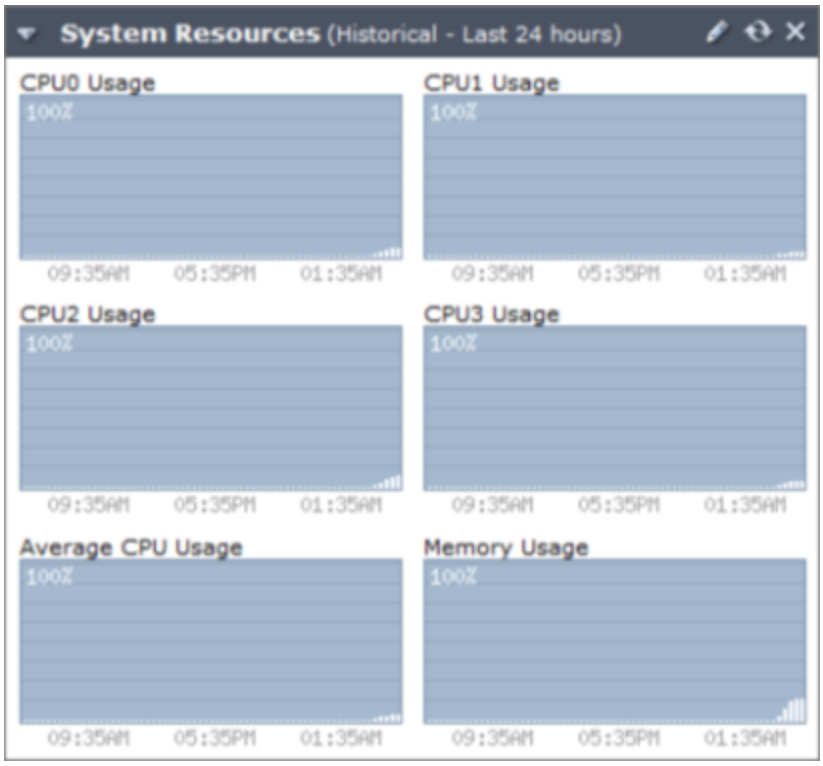
The following information is available on this widget:

Port numbers (vary depending on model)	The image below the port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection. For more information about a port's configuration and throughput, position your mouse over the icon for that port. A pop-up box displays the full name of the interface, the IP address and netmask, the status of the link, the speed of the interface, and the number of sent and received packets.
Reboot	Select to restart the FortiAnalyzer unit. You are prompted to confirm before the reboot is executed.
Shutdown	Select to shutdown the FortiAnalyzer unit. You are prompted to confirm before the shutdown is executed.

System Resources widget

The System Resources widget on the dashboard displays the usage status of the CPU, memory and hard disk. You can view system resource information in real-time or historical format, and either the average CPU usage or the usage for each individual processor core.





The following information is available:

CPUx Usage	The current CPU utilization for each processor core. The GUI displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the GUI) is excluded.
Average CPU Usage	The current average CPU utilization. The GUI displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the GUI) is excluded.
Memory Usage	The current memory utilization. The GUI displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the GUI) is excluded.
Hard Disk Usage	The current hard disk usage, shown on a pie chart as a percentage of total hard disk space. This item does not appear when viewing historical system resources.

To change the system resource widget display settings:

1. Go to *System Settings* > *Dashboard*.
2. In the System Resources widget, hover the mouse over the title bar and select the *Edit* icon. The *Edit System Resources Settings* dialog box appears.

3. You can configure the following settings:

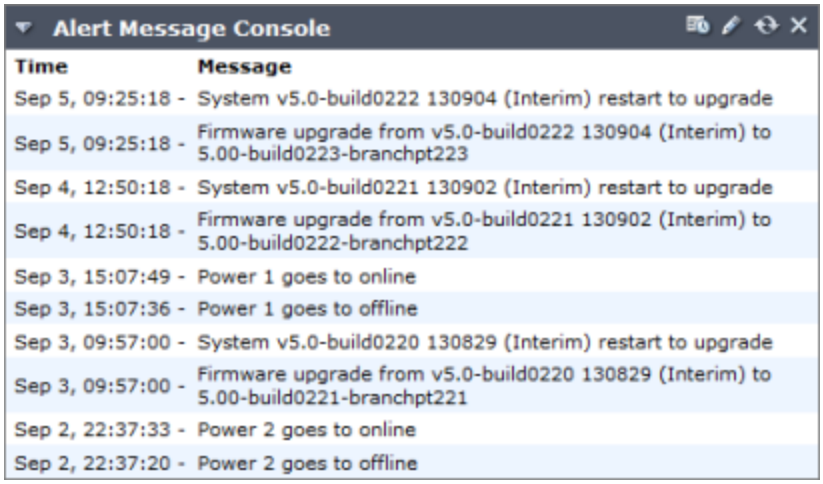
Multi-core CPU Display	Select *Each Core* to view the CPU usage for each processor core (default). Select *Average* to view only the average CPU usage.
View Type	Select *Real Time* to view the most current information about system resources (default). Select *Historical* to view historical information about system resources.
Time Period	Select one of the following: *Last 10 minutes*, *Last 1 hour,* or *Last 24 hours*. This option is only available when *Historical* is selected.
Refresh Interval	To automatically refresh the widget at intervals, enter a number between 10 and 240 seconds. To disable the refresh interval feature, enter *0*.

4. Select *OK* to apply your settings.

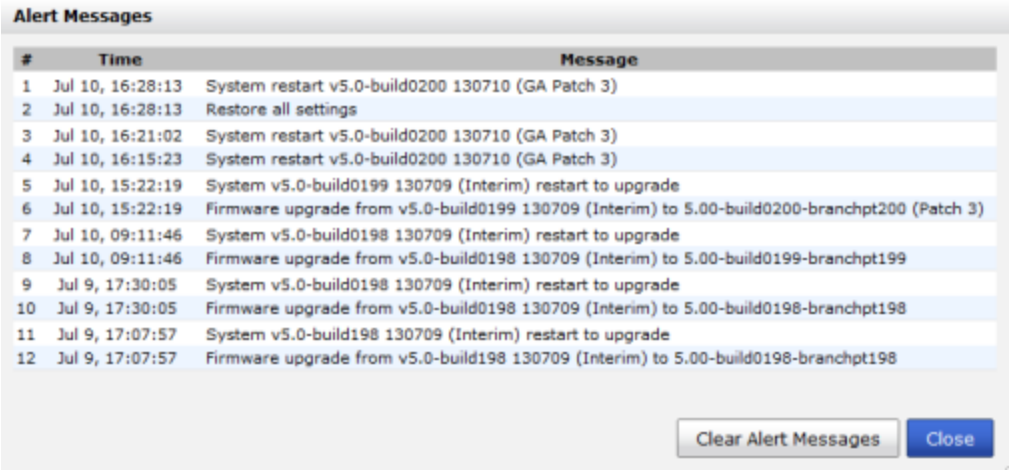
Alert Messages Console widget

The Alert Message Console widget displays log-based alert messages for both the FortiAnalyzer unit itself and connected devices.

Alert messages help you track system events on your FortiAnalyzer unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time that the event occurred.



The widget displays only the most recent alerts. For a complete list of unacknowledged alert messages, select the *More Alerts* icon in the widget's title bar. A popup window appears. To clear the list, select *Clear Alert Messages*.



Select the *Edit* icon in the title bar to open the *Edit Alert Message Console Settings* dialog box so that you can adjust the number of entries that are visible, and their refresh interval.

CLI Console widget

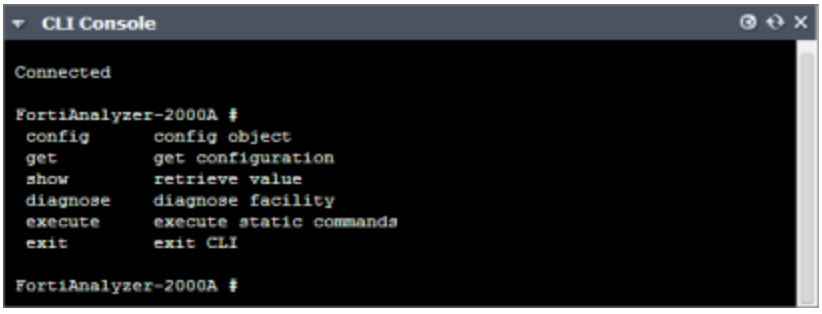
The CLI Console widget enables you to enter CLI commands through the GUI without making a separate Telnet, SSH, or local console connection.

The *CLI Console* widget requires that your web browser support JavaScript.

To use the console, click within the console area. Doing so will automatically log you in using the same administrator account that you used to access the GUI. You can then enter commands by typing them. You can also copy and paste commands in to or out of the console.

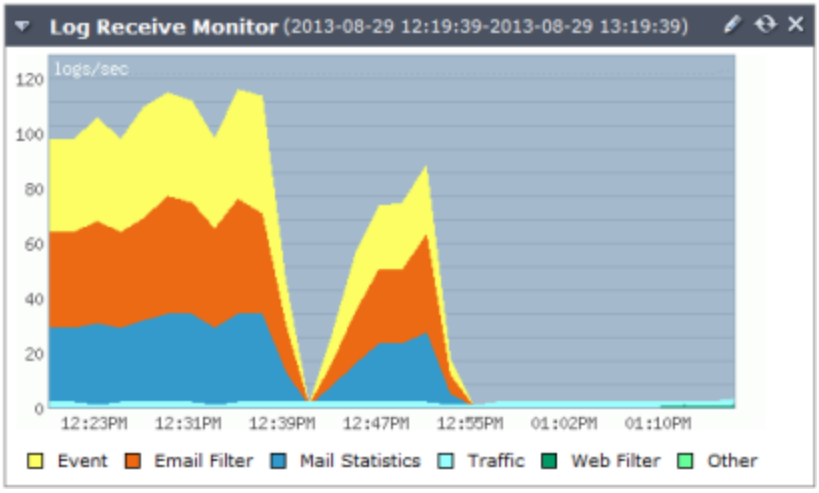
The command prompt contains the host name of the Fortinet unit (by default, the model number such as `Fortinet-800B #`). To change the host name, see Changing the host name on page 55.

For information on available CLI commands, see the FortiAnalyzer CLI Reference.



Log Receive Monitor widget

The Log Receive Monitor widget displays the rate at which logs are received over time. You can select to display log data by log type or per device.

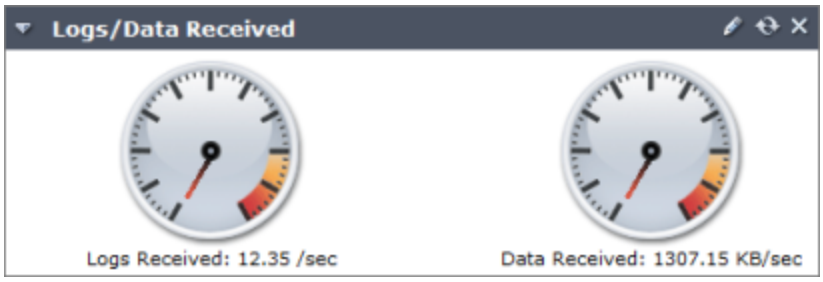


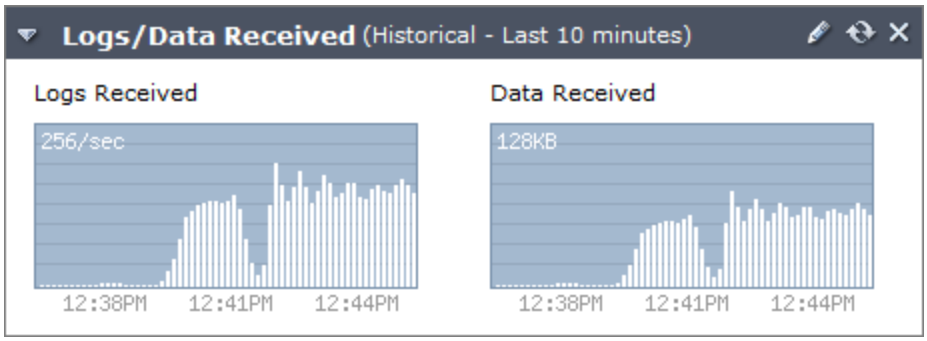
To configure settings for the widget, select *Edit* from the title bar, then configure the following settings in the *Edit Log Receive Monitor Settings* dialog box:

Type	From the drop-down menu, select either: • *Log Type*: Display the type of logs that are received from all registered devices separated into the following categories: *Event*, *Email Filter*, *Mail Statistics*, *Traffic*, *Web Filter*, and *Other*. • *Device*: Display the logs that received by each registered device separated into the top number of devices.
Number of Entries	Select the number of either log types or devices shown in the widget's graph.
Time Period	Select one of the following time ranges over which to monitor the rate at which log messages are received: *Hour*, *Day*, *Week*.
Refresh Interval	Automatically refresh the widget. Enter a number between 10 and 240 seconds. To disable automatic refresh, enter `0`.

Logs/Data Received widget

The Logs/Data Received widget displays the rate over time of the logs and data, such as Traffic, Web Filter, and Event logs, received by the FortiAnalyzer unit.





The widget displays the following information:

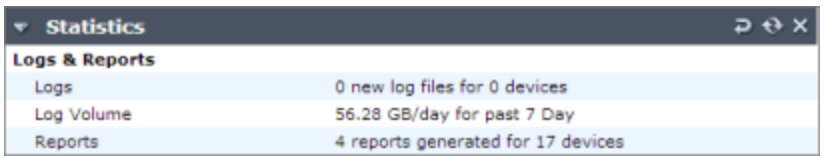
Logs Received	Number of logs received per second.
Data Received	Volume of data received.

To configure settings for the widget, select *Edit* from the title bar, then configure the following settings in the *Edit Logs/Data Received Settings* dialog box:

View Type	Select *Real Time* to view current information about system resources. Select *Historical* to view historical information.
Time Period	Select one of the following time ranges: *Last 10 Minutes*, *Last 1 Hour,* or *Last 24 Hours*.
Refresh Interval	Automatically refresh the widget. Enter a number between 10 and 240 seconds. To disable automatic refresh, enter `0`.

Statistics widget

The Statistics widget displays the numbers of sessions, volume of log files, and number of reports handled by the FortiAnalyzer unit.



The widget displays the following information:

Logs	The number of new log files received from a number of devices since the statistics were last reset.
Log Volume	The average log file volume received per day over the past seven days.
Reports	The number of reports generated for a number of devices.
Reset	Select *Reset* to reset the aforementioned statistics back to zero.

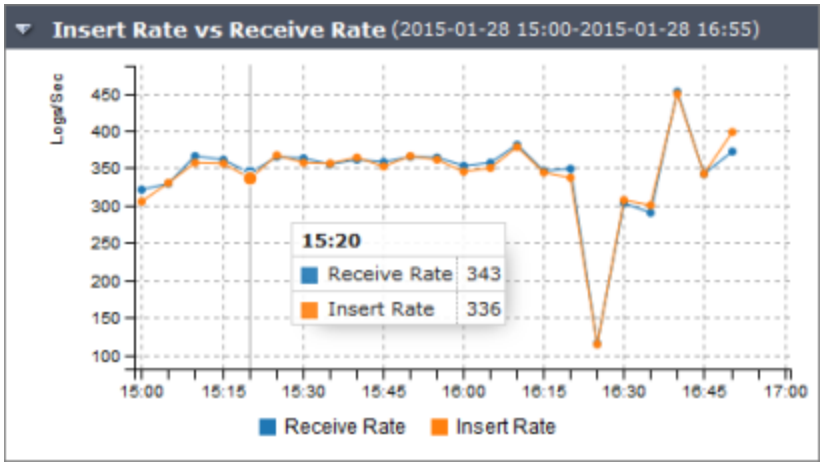
Insert Rate vs Receive Rate widget

The Insert Rate vs Receive Rate widget displays the log insert and log receive rates in a line graph.

- Log receive rate: how many logs are being received.
- Log insert rate: how many logs are being actively inserted into the datebase.

If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs that are waiting to be inserted.

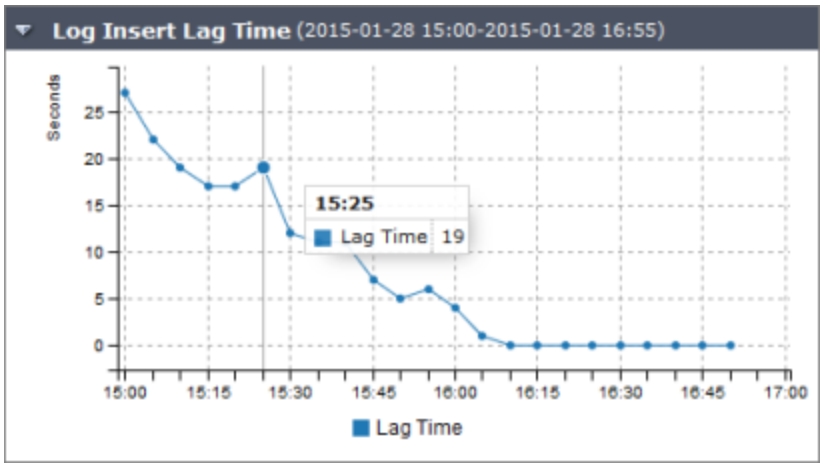
Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted and a specific time.



Select the edit icon in the widget toolbar to adjust the time interval shown on the graph (last 1 hour, 8 hours, or 24 hours) and the refresh interval (60 - 240 seconds, 0 to disable) of the widget.

Log Insert Lag Time widget

The Log Insert Lag Time widget shows the how many seconds the database is behind in processing the logs.

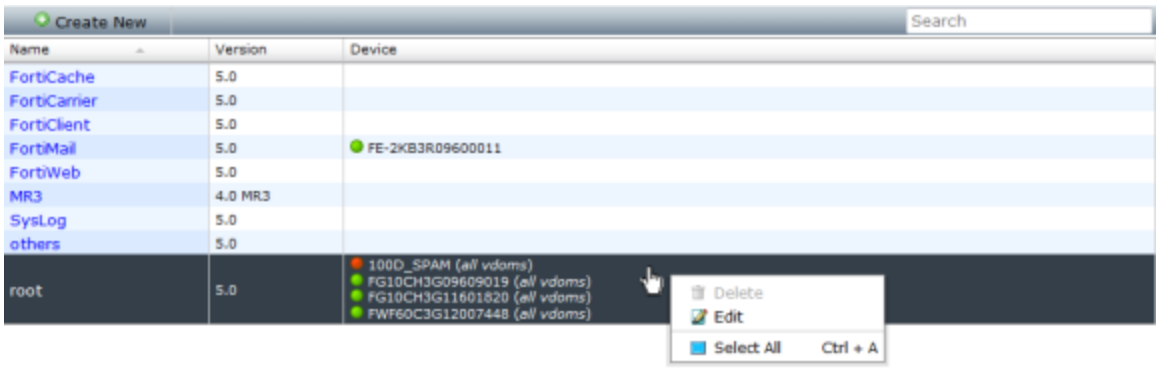


Select the edit icon in the widget toolbar to adjust the time interval shown on the graph (last 1 hour, 8 hours, or 24 hours) and the refresh interval (60 - 240 seconds, 0 to disable) of the widget.

All ADOMs

The *All ADOMs* menu item displays all the ADOMs configured on the device, and provides the option to create new ADOMs. It is only visible if ADOMs are enabled, see System Information widget on page 53.

FortiAnalyzer v5.0.7 and later supports FortiGate, FortiCache, FortiCarrier, FortiClient, FortiMail, FortiSandbox, FortiWeb, Syslog, and others ADOM types.



The following information and options are available:

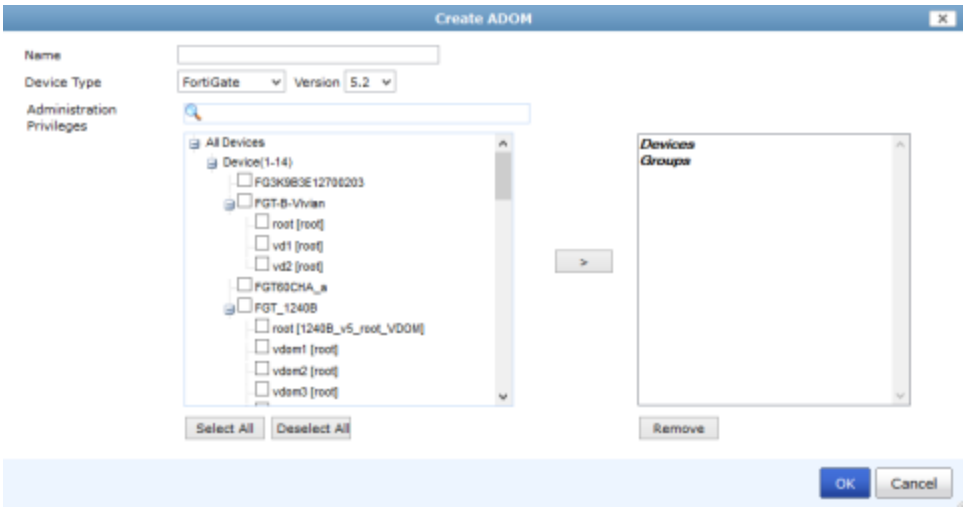
Create New	Select to create a new ADOM.
Search	Enter a keyword to search your ADOMs.
Name	The names of the current ADOMs.
Version	The firmware release version of the ADOM.
Device	The devices currently in the ADOM.

Right-click on an ADOM in the list to open the right-click menu. The following options are available:

Delete	Select *Delete* in the right-click menu to delete the ADOM.
Edit	Select *Edit* in the right-click menu to edit the ADOM.
Select All	Select *Select All* in the right-click menu to select all ADOMs in the list.

To create a new ADOM:

1. Select *Create New* from the ADOM list toolbar.
   The *Create ADOM* dialog box opens.



2. Enter a name for the ADOM in the *Name* field.
3. Select the device type and firmware version from the drop-down lists.
4. Select the devices to be added to the ADOM from the device list on the left, then select the arrow button to transfer them into the selected devices list on the right.
5. Select *OK* to create the ADOM.

To edit an ADOM:

1. Right-click on the ADOM you need to edit and select *Edit* from the right-click menu, or double-click anywhere in the ADOM's row. The *Edit ADOM* dialog box opens.
2. Edit the ADOM information as required and then select *OK*.
   The device type and version cannot be edited.

The default ADOMs cannot be edited.

To disable an ADOM:

1. Right-click on the ADOM you need to disable and select *Edit* from the right-click menu, or double-click anywhere in the ADOM's row. The *Edit ADOM* dialog box opens.

2. Uncheck the *Status* checkbox and then select *OK*.
   You must remove all devices before disabling the ADOM.

To delete an ADOM:

1. Right-click on the ADOM you would like to delete and select *Delete* from the right-click menu.
2. Select *OK* in the confirmation dialog box to delete the ADOM.

The default ADOMs cannot be disabled or deleted.

RAID management

RAID helps to divide data storage over multiple disks, providing increased data reliability. FortiAnalyzer units that contain multiple hard disks can have their RAID array configured for capacity, performance, and availability.

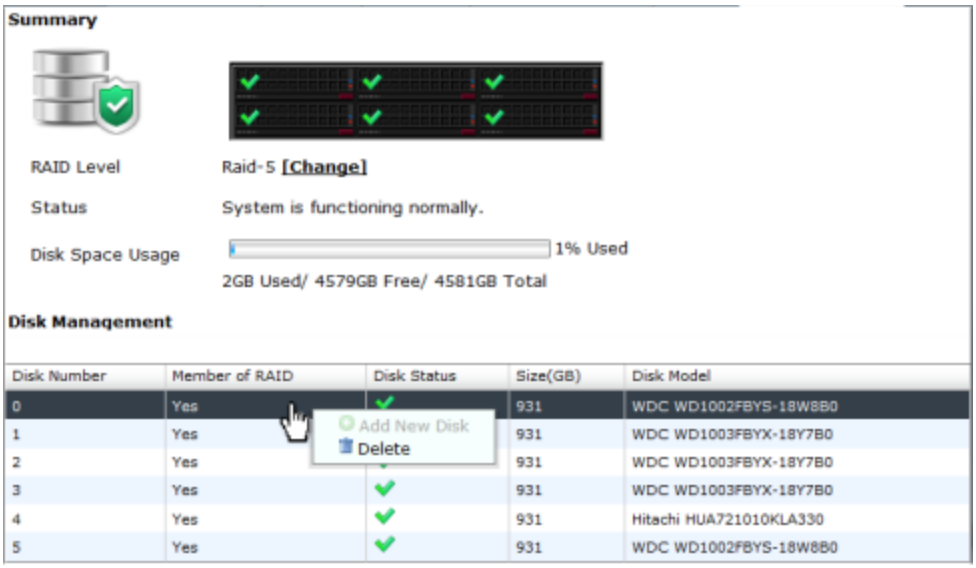
This menu is only available on devices that support RAID.

You can view the status of the RAID array from the RAID menu in *System Settings* > *RAID Management*. The RAID Management page displays the status of each disk in the RAID array, including the disk's RAID level. This menu also displays how much disk space is being used.

Under *Disk Management* the following information is displayed: *Disk Number*, *Member of RAID*, *Disk Status*, *Size (GB)*, and *Disk Model*.

The *Alert Message Console* widget, located in *System Settings*> *Dashboard*, will provides detailed information about any RAID array failures. For more information see Alert Messages Console widget on page 61.

If you need to remove a disk from the FortiAnalyzer unit, you might be able to hot swap it. Hot swapping means that you remove a failed hard disk and replace it with a new one while the FortiAnalyzer unit is in operation. Hot swapping is a quick and efficient way to replace hard disks. For more information about hot swapping, see Hot swapping hard disks on page 72.



To configure the RAID level:

1. Go to *System Settings* > *RAID Management*, in the *RAID Level* field, select *Change*. The *RAID Settings* dialog box opens.
2. From the *RAID Level* drop-down list, select the RAID level you want to use, then select *OK*. Once selected, depending on the RAID level, it may take a significant amount of time to generate the RAID array.

If the RAID settings is changed, all data will be deleted.

Supported RAID levels

FortiAnalyzer units with multiple hard drives can support the following RAID levels:

- **Linear**

  Linear RAID combines all hard disks into one large virtual disk. The total space available in this option is the capacity of all disks used. There is very little performance change when using this RAID format. If any of the drives fails, the entire set of drives is unusable until the faulty drive is replaced. All data will be lost.

- **RAID 0**

  A RAID 0 array is also referred to as striping. The FortiAnalyzer unit writes information evenly across all hard disks. The total space available is that of all the disks in the RAID array. There is no redundancy available. If any single drive fails, the data on that drive cannot be recovered. This RAID level is beneficial because it provides better performance, since the FortiAnalyzer unit can distribute disk writing across multiple disks.

  Minimum number of drives: 2

  Data protection: No protection

RAID 0 is not recommended for mission critical environments as it is not fault-tolerant.

- **RAID 1**

A RAID 1 array is also referred to as mirroring. The FortiAnalyzer unit writes information to one hard disk, and writes a copy (a mirror image) of all information to all the other hard disks. The total disk space available is that of only one hard disk, as the others are solely used for mirroring. This provides redundant data storage with no single point of failure. Should any of the hard disks fail, there are backup hard disks available.

Minimum number of drives: 2

Data protection: Single-drive failure

One write or two reads are possible per mirrored pair. RAID 1 offers redundancy of data. A re-build is not required in the event of a drive failure. This is the simplest RAID storage design with the highest disk overhead.

- **RAID 1 +Spare**

  A RAID 1 with hot spare (or RAID 1s) array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure, the hot spare is substituted for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk becomes the new hot spare.

- **RAID 5**

  A RAID 5 array employs striping with a parity check. Similar to RAID 0, the FortiAnalyzer unit writes information evenly across all drives but additional parity blocks are written on the same stripes. The parity block is staggered for each stripe. The total disk space is the total number of disks in the array, minus one disk for parity storage. For example, with four hard disks, the total capacity available is actually the total for three hard disks. RAID 5 performance is typically better with reading than with writing, although performance is degraded when one disk has failed or is missing. With RAID 5, one disk can fail without the loss of data. If a drive fails, it can be replaced and the FortiAnalyzer unit will restore the data on the new disk by using reference information from the parity volume.

  Minimum number of drives: 3

  Data protection: Single-drive failure

- **RAID 5 +Spare**

  A RAID 5 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure, the hot spare is substituted for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk becomes the new hot spare.

- **RAID 6**

  A RAID 6 array is the same as a RAID 5 array with an additional parity block. It uses block-level striping with two parity blocks distributed across all member disks.

  Minimum number of drives: 4

  Data protection: Up to two disk failures.

- **RAID 6 +Spare**

  A RAID 6 with hot spare array is the same as a RAID 5 with hot spare array with an additional parity block.

- **RAID 10**

  RAID 10 (or 1+0), includes nested RAID levels 1 and 0, or a stripe (RAID 0) of mirrors (RAID 1). The total disk space available is the total number of disks in the array (a minimum of 4) divided by 2, for example:

- two RAID 1 arrays of two disks each
- three RAID 1 arrays of two disks each
- six RAID1 arrays of two disks each.

One drive from a RAID 1 array can fail without the loss of data; however, should the other drive in the RAID 1 array fail, all data will be lost. In this situation, it is important to replace a failed drive as quickly as possible.

Minimum number of drives: 4

Data protection: Up to two disk failures in each sub-array.

Alternative to RAID 1 when additional performance is required.

- **RAID 50**

  RAID 50 (or 5+0) includes nested RAID levels 5 and 0, or a stripe (RAID 0) and stripe with parity (RAID 5). The total disk space available is the total number of disks minus the number of RAID 5 sub-arrays. RAID 50 provides increased performance and also ensures no data loss for the same reasons as RAID 5. One drive in each RAID 5 array can fail without the loss of data.

  Minimum number of drives: 6

  Data protection: Up to one disk failure in each sub-array.

Higher fault tolerance than RAID 5 and higher efficiency than RAID 0.

RAID 50 is only available on models with 9 or more disks. By default, two groups are used unless otherwise configured via the CLI. Use the `diagnose system raid status` CLI command to view your current RAID level, status, size, groups, and hard disk drive information.

- **RAID 60**

  A RAID 60 (6+0) array combines the straight, block-level striping of RAID 0 with the distributed double parity of RAID 6.

  Minimum number of drives: 8

  Data protection: Up to two disk failures in each sub-array.

High read data transaction rate, medium write data transaction rate, and slightly lower performance than RAID 50.

RAID support per FortiAnalyzer model

Model	RAID Type	RAID Level	Hot Swappable
FAZ-100C	-	-	-
FAZ-200D	-	-	-

Model	RAID Type	RAID Level	Hot Swappable
FAZ-300D	Software RAID	Linear, 0, 1	No
FAZ-400C	-	-	-
FAZ-1000C	Software RAID	Linear, 0, 1, 10	No
FAZ-1000D	Software RAID	Linear, 0, 1, 10	No
FAZ-3000D	Hardware RAID	0, 1, 1 +Spare, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-3000E	Hardware RAID		Yes
FAZ-3500E	Hardware RAID		Yes
FAZ-3900E	Hardware RAID		Yes
FAZ-4000B	Hardware RAID	0, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-VM	-	-	-
FAZ-VM64, FAZ-VM64-HV	-	-	-

RAID disk status

The RAID management page displays the status of each disk in the RAID array. The possible disk states are:

- *OK*: The hard drive is functioning normally.
- *Rebuilding*: The FortiAnalyzer unit is writing data to a newly added hard drive in order to restore the hard drive to an optimal state. The FortiAnalyzer unit is not fully fault tolerant until rebuilding is complete.
- *Initializing*: The FortiAnalyzer unit is writing to all the hard drives in the device in order to make the array fault tolerant.
- *Verifying*: The FortiAnalyzer unit is ensuring that the parity data of a redundant drive is valid.
- *Degraded*: The hard drive is no longer being used by the RAID controller.
- *Inoperable*: One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system. Data on an inoperable drive cannot be accessed.

Hot swapping hard disks

If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the FortiAnalyzer unit is still running, known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget (see Alert Messages Console widget on page 61).

To hot-swap a hard disk on a device that supports hardware RAID, simply remove the faulty hard disk and replace it with a new one.

Electrostatic discharge (ESD) can damage FortiAnalyzer equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiAnalyzer chassis.
When replacing a hard disk, you need to first verify that the new disk has the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiAnalyzer unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.
The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

The FortiAnalyzer unit will automatically add the new disk to the current RAID array. The status appears on the console. The RAID management page will display a green check mark icon for all disks and the *RAID Status* area will display the progress of the RAID re-synchronization/rebuild.

Once a RAID array is built, adding another disk with the same capacity will not affect the array size until you rebuild the array by restarting the FortiAnalyzer unit.

Adding new disks

Some FortiAnalyzer units have space to add more hard disks to increase your storage capacity.

Fortinet recommends that you use the same disks as those supplied by Fortinet. Disks of other brands will not be supported by Fortinet. For information on purchasing extra hard disks, contact your Fortinet reseller.

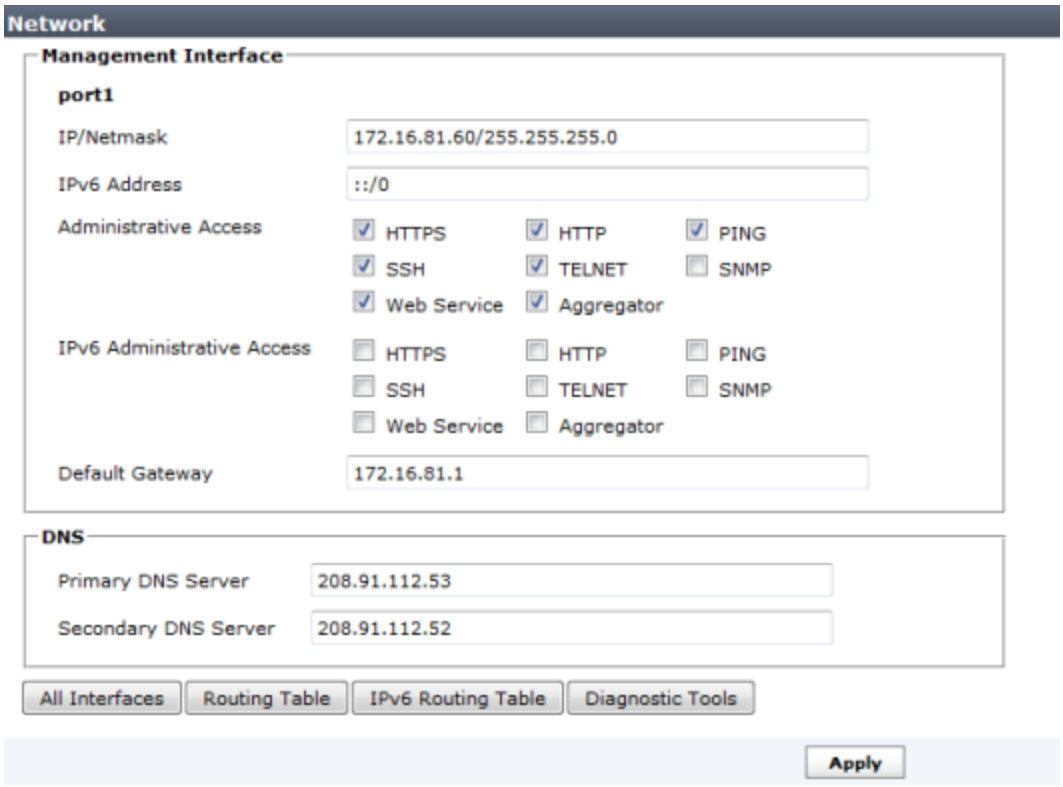
To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiAnalyzer unit. You can also migrate the data to another FortiAnalyzer. unit if you have one. Data migration reduces system down time and risk of data loss.
   For information on data backup, see Backing up the system on page 56
3. If your device has hardware RAID, install the disks in the FortiAnalyzer unit while the FortiAnalyzer unit is running.
   If your device has software RAID, shutdown the device (see Shutdown on page 59), install the disk or disks, then restart the device.
4. Configure the RAID level. If you have backed up the log data, restore the data. For more information, see Restoring the configuration on page 57.

Network

The FortiAnalyzer unit can manage Fortinet devices connected to any of its interfaces. The DNS servers must be on the networks to which the FortiAnalyzer unit connects, and should have two different addresses.

To view the configured network interfaces, go to *System Settings* > *Network*. The network screen is displayed.



Configure the following settings:

Management Interface		
	IP/Netmask	The IP address and netmask associated with this interface.
	IPv6 Address	The IPv6 address and netmask associated with this interface.
	Administrative Access	Select the allowed administrative service protocols from: *HTTPS*, *HTTP*, *PING*, *SSH*, *TELNET*, *SNMP*, *Web Service*, and *Aggregator*.
	IPv6 Admin-istrative Access	Select the allowed IPv6 administrative service protocols from: *HTTPS*, *HTTP*, *PING*, *SSH*, *TELNET*, *SNMP*, *Web Service*, and *Aggregator*.
	Default Gateway	The default gateway associated with this interface
DNS		

Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.
All Interfaces	Click to open the network interface list. See Network interfaces on page 75.
Routing Table	Click to open the routing table. See Static routes on page 76.
IPv6 Routing Table	Click to open the IPv6 routing table. See Static routes on page 76.
Diagnostic Tools	Select to run available diagnostic tools, including *Ping*, *Traceroute*, and *View logs*. See Diagnostic tools on page 77.

Network interfaces

To view the Network interface list, select the *All Interfaces* button.

The following information is displayed:

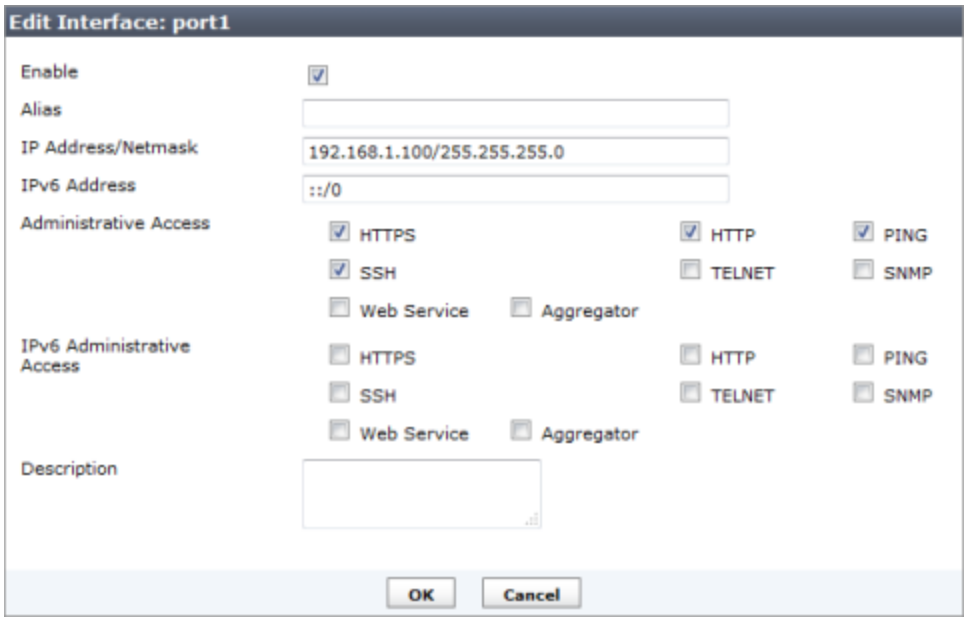
Name	The names of the physical interfaces on your FortiAnalyzer unit. The name of a physical interface depends on the model. Unlike FortiGate, you cannot set alias names for the interfaces. If HA operation is enabled, the HA interface has */HA* appended to its name.
IP/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Description	A description of the interface.
Administrative Access	The list of allowed administrative service protocols on this interface.
IPv6 Administrative access	The list of allowed IPv6 administrative service protocols on this interface.
Enable	Displays an enabled icon if the interface is enabled or a disabled icon if the interface is disabled.

The following options are available by right-clicking on a port:

Edit	Right-click on an interface and select *Edit* in the in the pop-up menu. Alternatively, double-click the entry to open the *Edit Interface* page.
Delete	Right-click on an interface and select *Delete* in the pop-up menu to remove the entry. Select *OK* in the confirmation dialog box to complete the delete action.

Configuring network interfaces

In the Network Interface list, select an interface name to change the interface options.



Configure the following settings, then select *OK* to apply your changes:

Enable	Select to enable this interface. An enabled icon appears in the interface list to indicate the interface is accepting network traffic. When not selected, a disabled icon appears in the interface list to indicate the interface is down and not accepting network traffic.
Alias	Enter an alias for the port to make it easily recognizable.
IP Address/Netmask	Enter the IP address and netmask for the interface.
IPv6 Address	Enter the IPv6 address for the interface.
Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiAnalyzer unit will require at least HTTPS or HTTP for GUI access, or SSH for CLI access.
IPv6 Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiAnalyzer unit will require at least HTTPS or HTTP for GUI access, or SSH for CLI access.
Description	Enter a brief description of the interface (optional).

Static routes

Go to *System Settings* > *Network*, select *Routing Table* to manage IPv4 static routes, or select *IPv6 Routing Table* to manage IPv6 static routes.

The following information is displayed:

ID	The route number.
IP/Netmask	The destination IPv4 address and netmask for this route.
IPv6 Address	The destination IPv6 address for this route (IPv6 Routing Table only).
Gateway	The address of the next hop router to which this route directs traffic.
Interface	The network interface that connects to the gateway.

The following options are available:

Create New	Select *Create New* to add a new route.
Delete	Select the check box next to the route number then select *Delete* to remove the route from the table. *Delete* is also available in the right-click menu.
Edit	Select from the right-click menu to open the *Edit Route* window.

Add a static route

Go to *System Settings* > *Network*, select *Routing Table* or *IPv6 Routing Table*, then select *Create New* to add a route, or select the route number to edit an existing route.

Configure the following settings, then select *OK* to create the new static route:

Destination	Enter the destination IP address and netmask, or IPv6 prefix, for this route.
Gateway	Enter the address of the next hop router to which this route directs traffic.
Interface	Select the network interface that connects to the gateway.

Diagnostic tools

Diagnostic tools allows you to run available diagnostic tools, including *Ping*, *Traceroute*, and *View logs*.

Admin

The *System Settings* > *Admin* menu enables you to configure administrator accounts, access profiles, and adjust global administrative settings for the FortiAnalyzer unit. The following sub-menu options are available:

Administrator	Select to configure administrative users accounts. For more information, see Administrator on page 79.

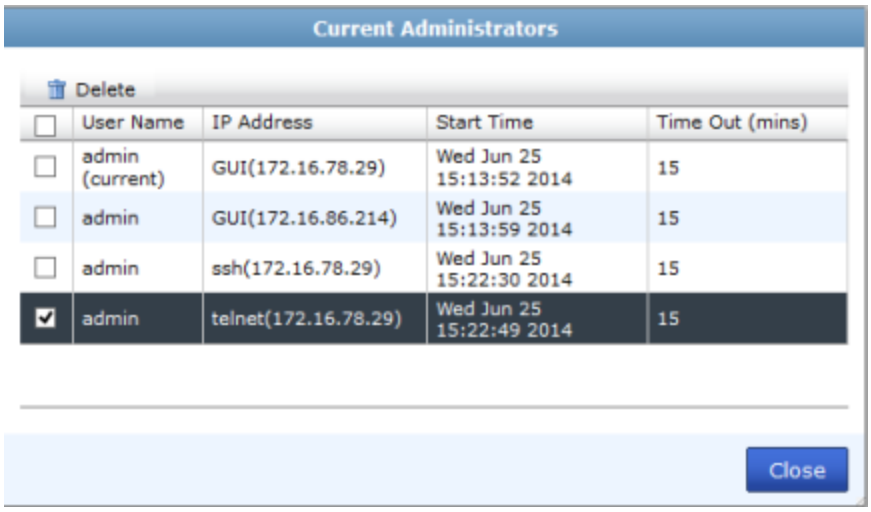
Profile	Select to set up access profiles for the administrative users. For more information, see Profile on page 82.
Remote Auth Server	Select to configure authentication server settings for administrative log in. For more information, see Remote authentication server on page 85.
Admin Settings	Select to configure connection options for the administrator including port number, language of the GUI and idle timeout. For more information, see Administrator settings on page 89.

Monitoring administrator sessions

The Current Administrators view enables you to view the list of administrators logged into the FortiAnalyzer unit. From this window you can also disconnect users if necessary.

To view logged in administrators on the FortiAnalyzer unit, go to *System Settings > Dashboard.* In the *System Information* widget, under *Current Administrators*, select *Detail*.

The list of current administrator sessions opens.



The following information is displayed:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The login type (GUI, jsconsole, SSH, telnet) and IP address where the administrator is logging in from.
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).
Delete	Select the check box next to the user and select *Delete* to drop their connection to the FortiAnalyzer unit. Select *OK* in the confirmation dialog box to proceed with the delete action.

To disconnect an administrator:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Current Administrators field*, select *Detail*. The list of current administrator sessions appears.
3. Select the check box for each administrator session that you want to disconnect, and select *Delete*.
4. Select *OK* to confirm deletion of the session.

   The disconnected administrator will see the FortiAnalyzer login screen when disconnected. They will not have any additional warning. If possible, it is advisable to inform the administrator before disconnecting them, in case they are in the middle of important configurations for the FortiAnalyzer or another device.

Administrator

Go to *System Settings* > *Admin* > *Administrator* to view the list of administrators and configure administrator accounts. Only the default `admin` administrator account can see the complete administrators list. If you do not have certain viewing privileges, you will not see the administrator list.

The following information is displayed:

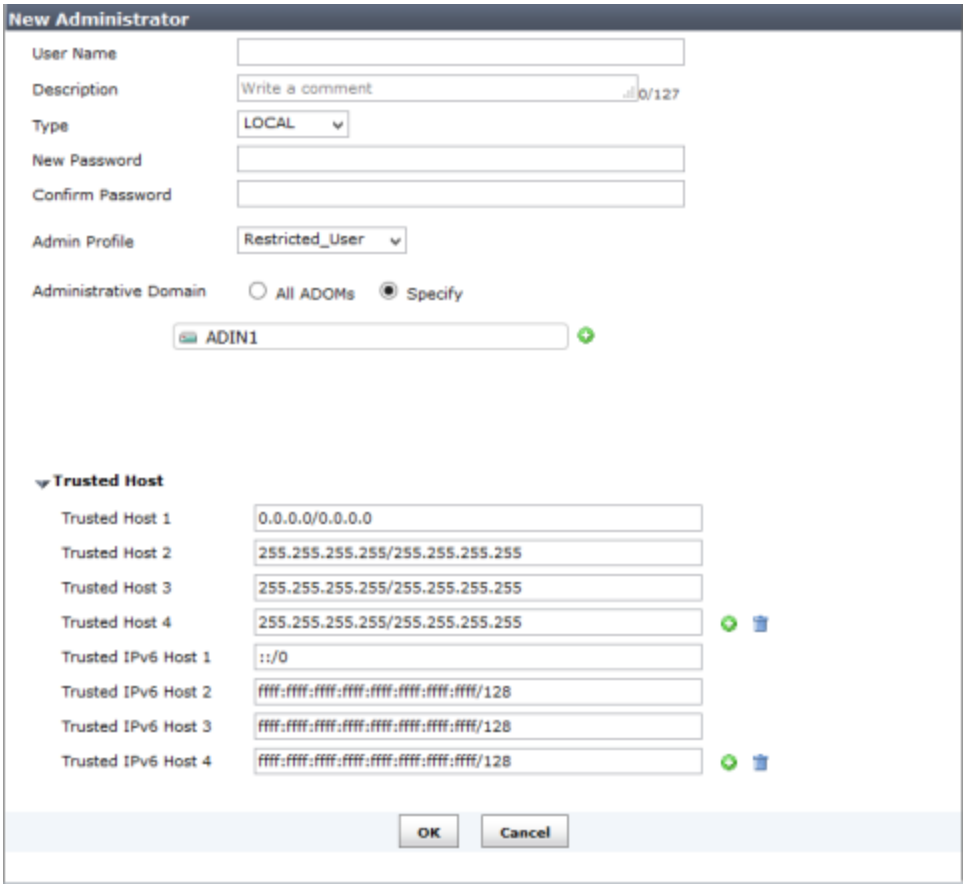
User Name	The name this administrator uses to log in. Select the administrator name to edit the administrator settings.
Type	The type of administrator account, one of: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, or *PKI*.
Profile	The administrator profile for this user that determines the privileges of this administrator. The profile can be one of: *Restricted_User*, *Standard_User*, *Super_User*, or a custom defined profile. For information on administrator profiles, see Profile on page 82.
ADOM	The ADOMs to which the user has access. ADOM access can be to all ADOMs or specific ADOMs which are assigned to the profile.
Status	Indicates whether the administrator is currently logged into the FortiAnalyzer unit not. A green circle with an up arrow indicates that the administrator is logged in, a red circle with a down arrow indicates that they are not.
Comments	Descriptive text about the administrator account.

The following options are available:

Create New	Select to create a new administrator.
Delete	Select the check box next to the administrator you want to remove from the list and select *Delete*. Delete is also available in the right-click menu.
Edit	Select the administrator in the table, right-click, and select *Edit* in the right-click menu to edit the entry. Alternatively, you can double-click the entry to open the *Edit Administrator* page.

To create a new administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New*. The *New Administrator* dialog box appears.



2. Configure the following settings:

User Name	Enter the name that this administrator uses to log in.
Description	Optionally, enter a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account.
Type	Select the type of authentication the administrator will use when logging into the FortiAnalyzer unit. Select one of: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, or *PKI*.
Subject	If *Type* is set to *PKI*, enter a description.
CA	If *Type* is set to *PKI*, select a certificate in the drop-down list.
Require two-factor authentication	If *Type* is set to *PKI*, you can select the checkbox to enforce two-factor authentication. Enter a password and confirm.
New Password	If *Type* is set to *Local*, enter a password.

Confirm Password	If *Type* is set to *Local*, enter the password again to confirm it.
Server	Select the *RADIUS*, *LDAP*, or *TACACS+* server, as appropriate. This option is only available if *Type* is not *LOCAL* or *PKI*.
wildcard	Select this option to set the password as a wildcard. This option is only available if *Type* is not *LOCAL* or *PKI*.
Admin Profile	Select a profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features. *Restricted_User* and *Standard_User* admin profiles do not have access to the *System Settings* tab. An administrator with either of these admin profiles will see a change password icon in the navigation pane. To create a new profile see Configuring administrator profiles on page 84.
Admin Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an Administrative Domain. This field is available only if ADOMs are enabled (see Administrative Domains on page 35).The *Super_User* profile defaults to *All ADOMs* access.
Trusted Host	Optionally, enter the trusted host IPv4 or IPv6 address and network mask from which the administrator can log in to the FortiAnalyzer unit. You can specify up to ten trusted hosts in the GUI or in the CLI. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 81.

3. Select *OK* to create the new administrator account.

To edit an administrator account:

1. From the administrator list, either double-click on an administrator, or right-click and select *Edit*. The *Edit Administrator* window opens.
2. Edit the settings as required.
3. Optionally, select *Change Password* to change the password associated with the account.
4. Select *OK* to save your changes.

To delete an existing administrator account:

1. From the administrator list, select the check box of the administrator account or accounts that you need to delete, then select *Delete* in the toolbar.
2. Select *OK* in the confirmation dialog box to delete the administrator account.

The default *admin* administrator account cannot be deleted.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the

subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiAnalyzer unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

If you set trusted hosts and want to use the Console Access feature of the GUI, you must also set 127.0.0.1/255.255.255.255 as a trusted host. By default, Trusted Host 3 is set to this address.

Profile

The profile list allows you to create and edit administrator profiles. Administrator profiles are used to limit administrator access privileges to devices or system features. The administrator profiles restrict access to both the GUI and CLI.

To view the list of administrator profiles, go to the *System Settings* > *Admin* > *Profile* page.

The following information is displayed:

Profile	The administrator profile name. Select the profile name to view or modify existing settings. For more information about profile settings, see Configuring administrator profiles on page 84.
Type	The profile type, which is always *System Admin*.
Description	Provides a brief description of the system and device access privileges allowed for the selected profile.

The following options are available:

Create New	Select to create a custom administrator profile. See To create a new profile: on page 84.
Delete	Select the check box next to the profile you want to delete and select *Delete*. Predefined profiles cannot be deleted. You can only delete custom profiles when they are not applied to any administrators. Delete is also available in the right-click menu. See To delete a profile: on page 84.
Edit	Right-click on a profile and select *Edit* in the right-click menu, or double-click on a profile to open the *Edit Profile* page. See To edit a profile: on page 84.

Predefined profiles

There are three predefined profiles:

Restricted_User	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.
Standard_User	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
Super_User	Super user profiles have all system and device privileges enabled.

Restricted_User and *Standard_User* admin profiles do not have access to the *System Settings* tab. An administrator with either of these admin profiles will see a change password icon in the navigation pane.

When *Read-Write* is selected, the user can view and make changes to the FortiAnalyzer system. When *Read-Only* is selected, the user can only view information. When *None* is selected, the user can neither view or make changes to the FortiAnalyzer system.

Feature	Predefined Administrator Profiles		
	Super User	Standard User	Restricted User
System Settings / `system-setting`	Read-Write	None	None
Administrator Domain / `adom-switch`	Read-Write	Read-Write	None
Device Manager / `device-manager`	Read-Write	Read-Write	Read-Only
Add/Delete Devices/Groups / `device-op`	Read-Write	Read-Write	None
FortiView / `realtime-monitor`	Read-Write	Read-Write	Read-Only
Log View / `log-viewer`	Read-Write	Read-Write	Read-Only
Reports / `report-viewer`	Read-Write	Read-Write	Read-Only
Event Management / `event-management`	Read-Write	Read-Write	Read-Only
CLI Only Settings			
`profileid`	Super_User	Standard_User	Restricted_User
`scope`	global	global	global

You cannot delete these profiles, but you can edit them. You can also create new profiles as required.

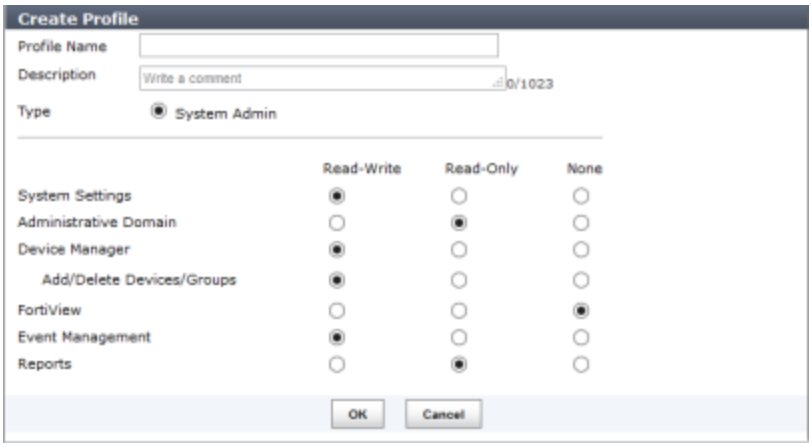
This guide is intended for default users with full privileges. If you create a profile with limited privileges it will limit the ability of any administrator using that profile to follow the procedures in this guide.

Configuring administrator profiles

You can create custom profiles, and edit existing profiles, including the predefined profiles, as required. Only administrators with full system privileges can edit the administrator profiles.

To create a new profile:

1. Go to *System Settings* > *Admin* > *Profile* and select *Create New*. The *Create Profile* dialog box opens.



2. Configure the following settings:

Profile Name	Enter a name for this profile.
Description	Enter a description for this profile. While not a requirement, a description can help to know what the profiles is for or the levels it is set to.
Type	This field is cannot be changed. The default type is *System Admin*.
Other Settings	Select *None*, *Read Only*, or *Read-Write* access for the categories as required.

3. Select *OK* to save the new profile.

To edit a profile:

1. From the profile list, right-click on a profile and select *Edit*, or double-click on a profile. The *Edit Profile* dialog box opens.
2. Edit the settings as required.
3. Select *OK* to save your changes.

The *Name* and *Type* fields cannot be changed when editing a profile in the GUI.

To delete a profile:

1. From the profile list, select the check box of the custom profile or profiles that you need to delete, then select *Delete* in the toolbar, or right-click on a profile and select *Delete*. You can only delete custom profiles that are not

applied to any administrators.

2. Select *OK* in the confirmation dialog box to delete the profile.

Remote authentication server

The FortiAnalyzer system supports remote authentication of administrators using Remote Authentication Dial-in User (RADIUS), Lightweight Directory Access Protocol (LDAP), and Terminal Access Controller Access-Control System (TACACS+) servers. To use this feature, you must configure the appropriate server entries in the FortiAnalyzer unit for each authentication server in your network. LDAP servers can be linked to all ADOMs or to specific ADOMs.

Go to *System Settings* > *Admin* > *Remote Auth Server* to view the server list.

The following information is displayed:

Name	The server name. Select the server name to edit the settings.
Type	The type of server, either LDAP, RADIUS, or TACACS+.
ADOM	The ADOM(s) that are associated with this server. This field is only applicable to LDAP servers.
Details	The IP address or DNS resolvable domain name of the server.

The following options are available:

Create New	Add a new LDAP, RADIUS, or TACACS+ server entry. See LDAP server on page 86, RADIUS server on page 87, and TACACS+ server on page 88.
Delete	Select the check box next to a server or servers then select *Delete*. You cannot delete a server entry if there are administrator accounts using it. Delete is also available in the right-click menu.
Edit	Right-click on a server and select *Edit*, or double-click on a server, to open the *Edit Server* page.

To edit a remote authentication server:

1. From the remote authentication server list, right-click on a server and select *Edit*, or double-click on a server, to open the *Edit Server* page. The appropriate edit window opens, depending on the server type selected.
2. Change the settings as required and select *OK* to apply your changes.

The *Name* field cannot be changed when editing a server configuration in the GUI.

To delete a server:

1. From the remote authentication server list, select the check box beside the server or servers that you need to delete and then select *Delete* from the toolbar, or right-click on a server and select *Delete*.
2. Select *OK* in the confirmation dialog box to delete the server entry.

You cannot delete a server entry if there are administrator accounts using it.

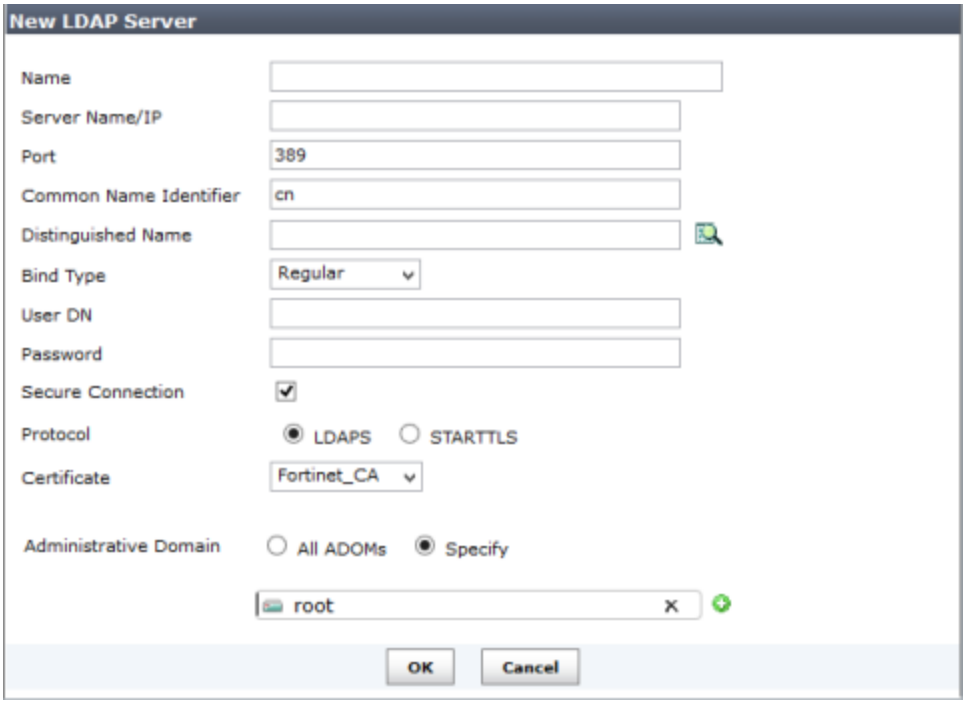
LDAP server

LDAP is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiAnalyzer unit contacts the LDAP server for authentication. To authenticate with the FortiAnalyzer unit, the user enters a user name and password. The FortiAnalyzer unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the FortiAnalyzer unit successfully authenticates the user. If the LDAP server cannot authenticate the user, the FortiAnalyzer unit refuses the connection.

To add an LDAP server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select the *Create New* toolbar and select *LDAP* in the drop-down list. The *New LDAP Server* dialog box opens.



3. Configure the following information:

Name	Enter a name to identify the LDAP server.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.

Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use *cn*. However, some servers use other common name identifiers such as *uid*.
Distinguished Name	The distinguished name used to look up entries on the LDAP servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Select the query icon to query the distinguished name.
Bind Type	Select the type of binding for LDAP authentication from the drop-down list. One of: *Simple*, *Anonymous*, or *Regular*.
User DN	Enter the user distinguished name. This option is available when the *Bind Type* is set to *Regular*.
Password	Enter the user password. This option is available when the *Bind Type* is set to *Regular*.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	Select either LDAPS or STARTTLS in the protocol field. This option is available when *Secure Connection* is selected.
Certificate	Select the certificate in the drop-down list. This option is available when *Secure Connection* is selected.
Administrative Domain	Select either *All ADOMs* or *Specify* to select which ADOMs to link to the LDAP server. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an Administrative Domain.

4. Select *OK* to save the new LDAP server entry.

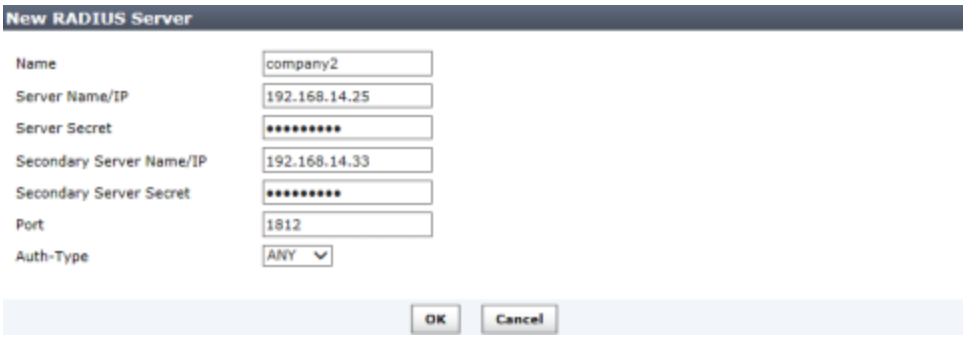
RADIUS server

RADIUS is a user authentication and network-usage accounting system. When users connect to a server they enter a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

You can create or edit RADIUS server entries in the RADIUS server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiAnalyzer unit uses the RADIUS server to verify the administrator password at logon. The password is not stored on the FortiAnalyzer unit.

To add a RADIUS server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select the *Create New* in the toolbar and select RADIUS in the drop-down list. The *New RADIUS Server* dialog box appears.



3. Configure the following settings:

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.
Server Secret	Enter the RADIUS server secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.
Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Auth-Type	Enter the authentication type the RADIUS server requires. Select from *ANY*, *PAP*, *CHAP*, or *MSv2 (MSCHAPv2)*. The default setting of *ANY* has the FortiAnalyzer unit try all the authentication types.

4. Select *OK* to save the new RADIUS server configuration.

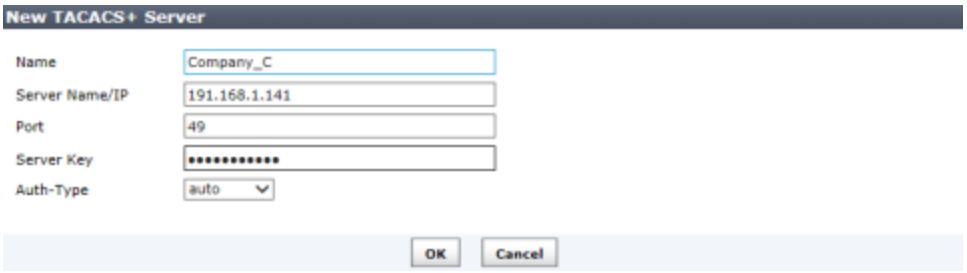
TACACS+ server

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS allows a client to accept a user name and password and send a query to a TACACS authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS server is 49.

For more information about TACACS+ servers, see the FortiGate documentation.

To add a TACACS+ server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select *Create New* in the toolbar and select TACACS+ in the drop-down list.



3. Configure the following information:

Name	Enter a name to identify the TACACS+ server.
Server Name/IP	Enter the IP address or fully qualified domain name of the TACACS+ server.
Port	Enter the port for TACACS+ traffic. The default port is *49*.
Server Key	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
Auth-Type	Enter the authentication type the TACACS+ server requires. Select one of: *auto*, *ASCII*, *PAP*, *CHAP*, or *MSCHAP*. The default value is *auto*.

4. Select *OK* to save the new TACACS+ server entry.

Administrator settings

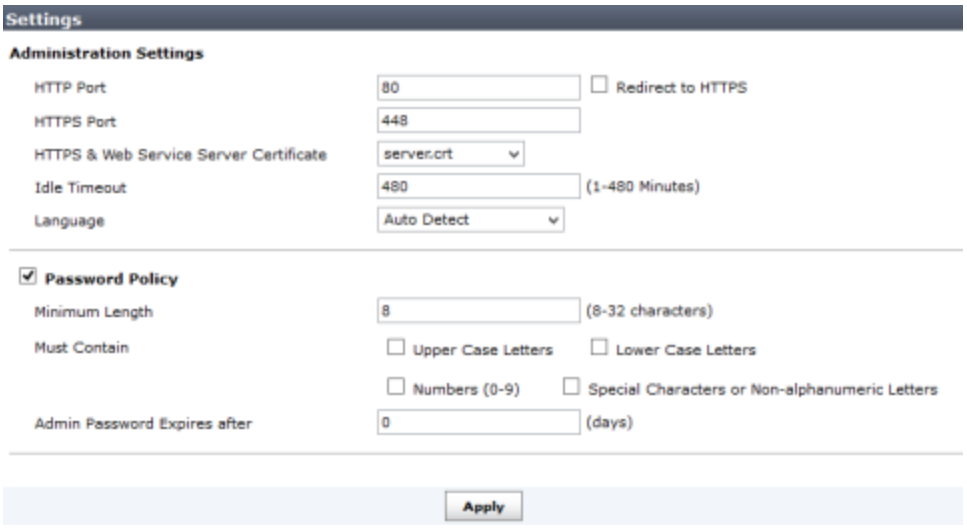
The *Admin Settings* page allows you to configure global settings for administrator access to the FortiAnalyzer unit, including:

- Ports for HTTPS and HTTP administrative access
- HTTPS & Web Service server certificate
- Idle Timeout settings
- Language of the GUI
- Password Policy

Only the`admin` administrator can configure these system options, which apply to all administrators logging onto the FortiAnalyzerunit.

To configure administrative settings:

1. Go to *System Settings* > *Admin* > *Admin Settings*. The *Settings* dialog box opens.



2. Configure the following settings:

Administration Settings		
	HTTP Port	Enter the TCP port to be used for administrative HTTP access.
	HTTPS Port	Enter the TCP port to be used for administrative HTTPS access.
	HTTPS & Web Service Server Certificate	Select a certificate from the drop-down list.
	Idle Timeout	Enter the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To ensure security, the idle timeout should be a short period of time to avoid the administrator inadvertently leaving the management computer logged in to the FortiAnalyzer unit, creating the possibility of someone walking up and modifying the network options.
	Language	Select a language from the drop-down list. Select either *English*, *Simplified Chinese*, *Traditional Chinese*, *Japanese*, *Korean*, or *Auto Detect*. The default value is *Auto Detect*.
Password Policy		
	Enable	Select to enable administrator passwords.
	Minimum Length	Select the minimum length for a password. The default is eight characters.
	Must Contain	Select the types of characters that a password must contain.
	Admin Password Expires after	Select the number of days that a password is valid for, after which time it must be changed.

3. Select *Apply* to save your settings. The settings are applied to all administrator accounts.

Configure two-factor authentication for administrator login

To configure two-factor authentication for administrator login you will need the following:

- FortiAnalyzer
- FortiAuthenticator
- FortiToken

FortiAuthenticator side configuration

The following instructions describes the steps required on your FortiAuthenticator device.

Before proceeding, ensure that you have configured your FortiAuthenticator and that you have created a NAS entry for your FortiAnalyzer and created/imported FortiTokens. For more information, see the *FortiAuthenticator Interoperability Guide* and *FortiAuthenticator Administration Guide* available in the Fortinet Document Library.

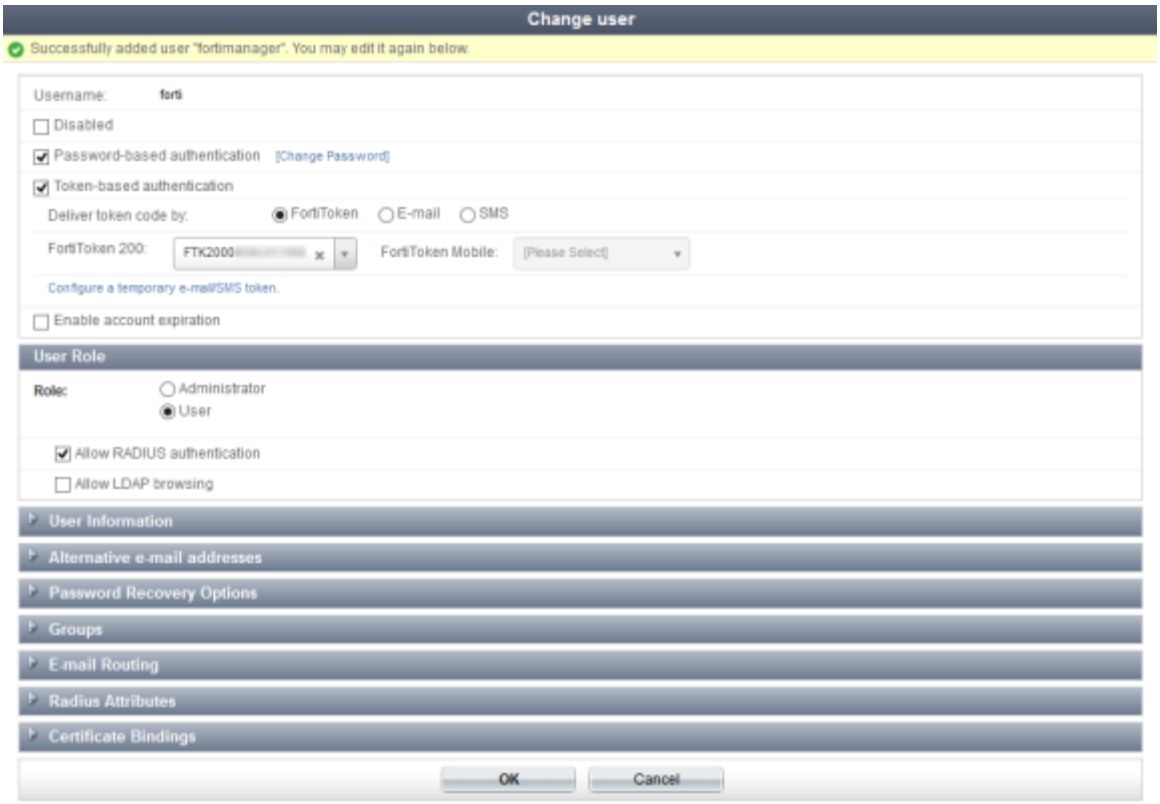
To create a new local user:

1. Go to *Authentication* > *User Management* > *Local Users*.
2. Select *Create New* in the toolbar. The *Create New User* page opens.

3. Configure the following settings:

Username	Enter a user name for the local user.
Password creation	Select Specify a password from the drop-down list.
Password	Enter a password. The password must be a minimum of 8 characters.
Password confirmation	Re-enter the password.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.

4. Select *OK* to continue. The *Change user* page opens.



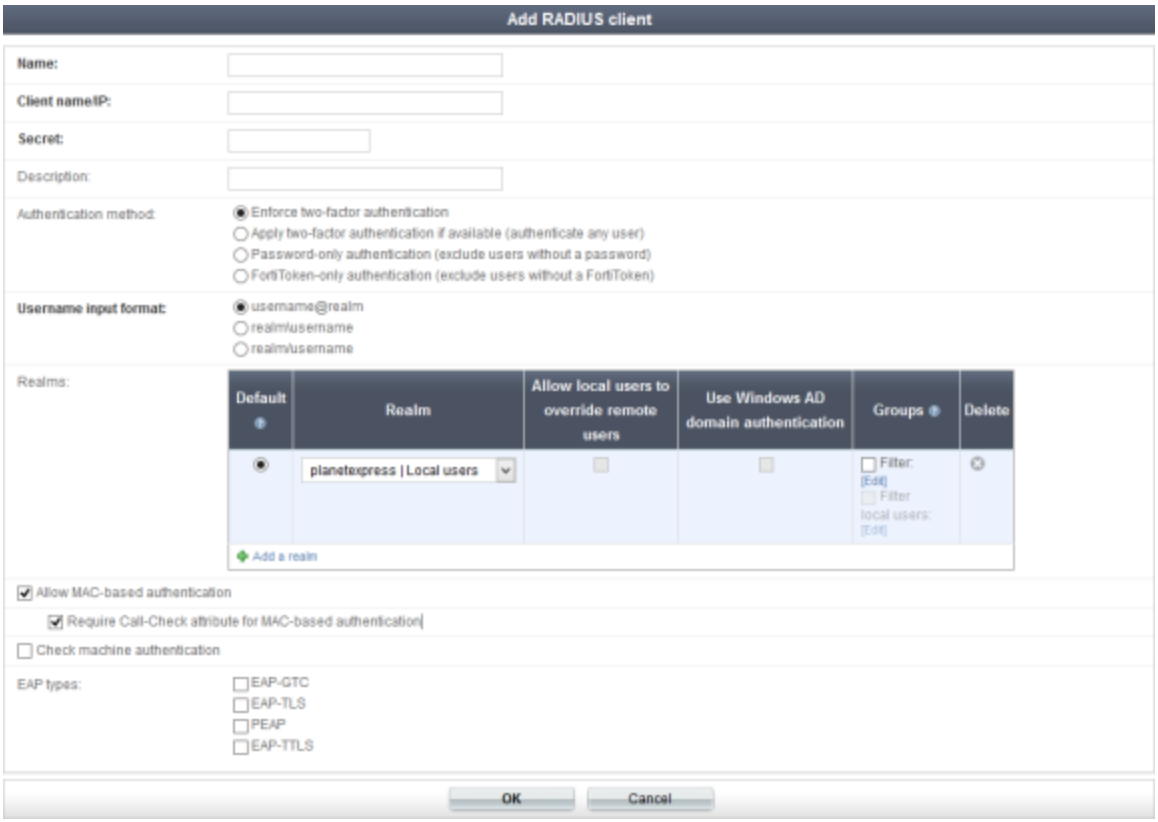
5. Configure the following settings:

Password-based authentication	Leave this option selected. Select *[Change Password]* to change the password for this local user.
Token-based authentication	Select to enable token-based authentication.
Deliver token code by	Select to deliver token by FortiToken.
FortiToken 200	Select the FortiToken from the drop-down list.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.
User Role	
Role	Select either Administrator or User.
Allow RADIUS authentication	Select to allow RADIUS authentication.
Allow LDAP browsing	Optionally, select to allow LDAP browsing. For more information see the *FortiAuthenticator Administration Guide*.

6. Select *OK* to save the setting.

To create a new RADIUS client:

1. Go to *Authentication* > *RADIUS Service* > *Clients*.
2. Select *Create New* in the toolbar. The *Create New RADIUS Client* page opens.



3. Configure the following settings:

Name	Enter a name for the RADIUS client entry.
Client name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiAnalyzer.
Secret	Enter the server secret. This value must match the FortiAnalyzer RADIUS server setting at *System Settings* > *Admin* > *Remote Auth Server*.
Description	Enter an option description for the RADIUS client entry.
Authentication method	Select *Enforce two-factor authentication* from the list of options.
Username input format	Select the username input format.
Realms	Create and define the Realm. For more information see the *FortiAuthenticator Administration Guide*.
Allow MAC-based authentication	Optional configuration. For more information see the *FortiAuthenticator Administration Guide*.

EAP types	Optional configuration. For more information see the *FortiAuthenticator Administration Guide*.

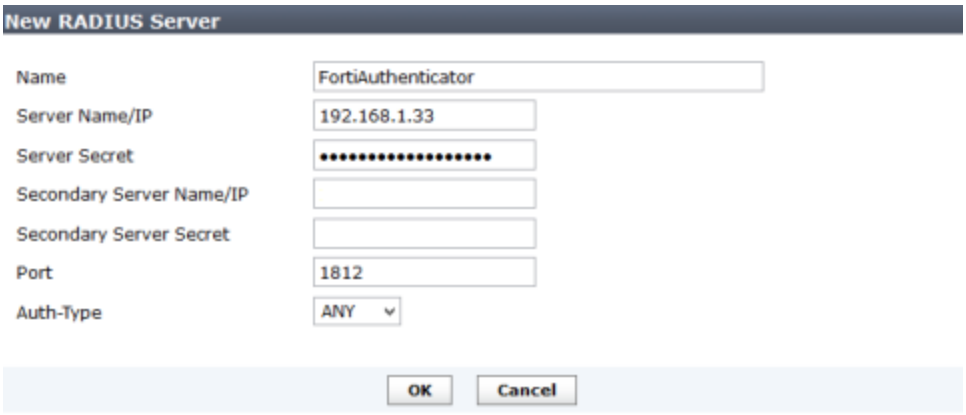
4. Select *OK* to save the setting.

FortiAnalyzer side configuration

The following instructions describes the steps required on your FortiAnalyzer device.

To configure the RADIUS server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select *Create New* in the toolbar and select *RADIUS* from the drop-down list. The *New RADIUS Server* page opens.



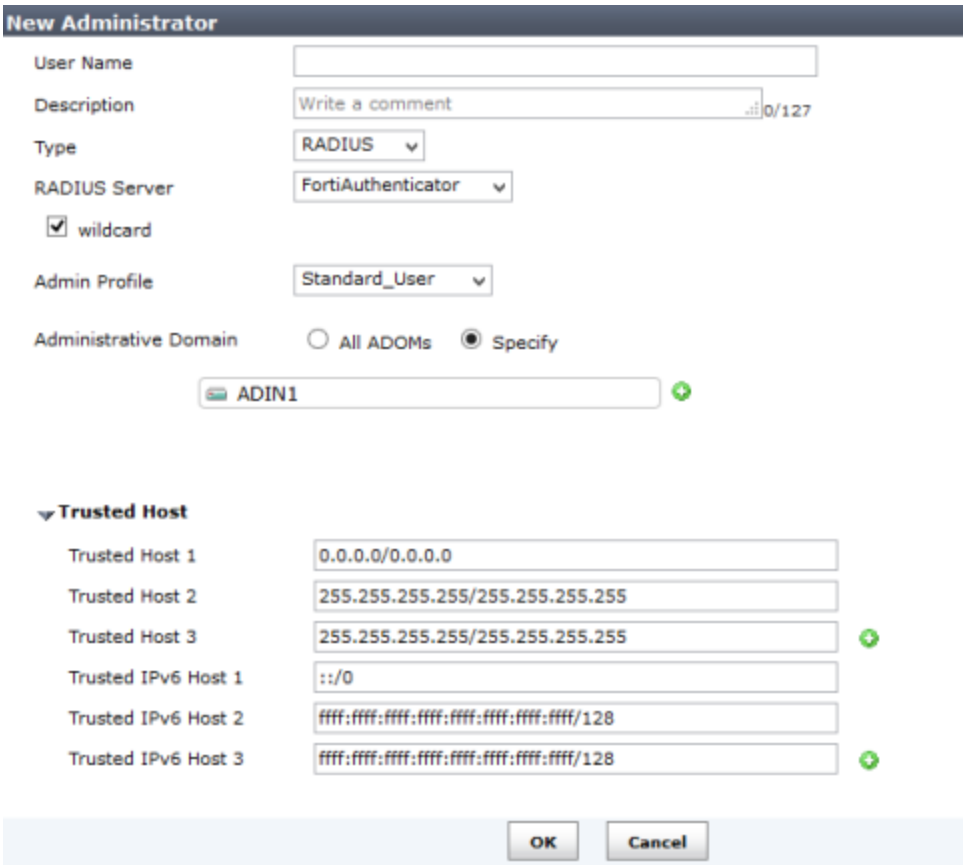
3. Configure the following settings:

Name	Enter a name to identify the FortiAuthenticator.
Server Name/IP	Enter the IP address or fully qualified domain name of your FortiAuthenticator.
Server Secret	Enter the FortiAuthenticator secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
Secondary Server Secret	Enter the secondary FortiAuthenticator secret, if applicable.
Port	Enter the port for FortiAuthenticator traffic. The default port is 1812.
Auth-Type	Enter the authentication type the FortiAuthenticator requires. The default setting of *ANY* has the FortiAnalyzer unit try all the authentication types. Select one of: *ANY*, *PAP*, *CHAP*, or *MSv2*.

4. Select *OK* to save the setting.

To create the admin users:

1. Go to *System Settings* > *Admin* > *Administrator*.
2. Select *Create New* in the toolbar. The *New Administrator* page opens.



3. Configure the following settings:

User Name	Enter the name that this administrator uses to log in.
Description	Optionally, enter a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account.
Type	Select RADIUS from the drop-down list.
RADIUS Server	Select the RADIUS server from the drop-down menu.
Wildcard	Select to enable wildcard. Wildcard authentication will allow authentication from any local user account on the FortiAuthenticator. To restrict authentication, RADIUS service clients can be configured to only authenticate specific user groups.
New Password	Enter the password. This field is available if *Type* is *RADIUS* and Wildcard is not selected.

Confirm Password	Enter the password again to confirm it. This field is available if *Type* is *RADIUS* and Wildcard is not selected.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's access to the FortiAnalyzer unit's features.To create a new profile see Configuring administrator profiles on page 84.
Administrative Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an Administrative Domain.This field is available only if ADOMs are enabled (see Administrative Domains on page 35).The *Super_User* profile defaults to *All ADOMs* access.
Trusted Host	Optionally, enter the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiAnalyzer unit. Select the add icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 81.

4. Select *OK* to save the setting.

To test the configuration:

1. Attempt to log into the FortiAnalyzer GUI with your new credentials.
2. Enter your user name and password and select *Login*. The FortiToken page is displayed.
3. Enter your FortiToken pin code and select *Submit* to finish logging in to FortiAnalyzer.

Certificates

The FortiAnalyzer unit generates a certificate request based on the information you enter to identify the FortiAnalyzer unit. After you generate a certificate request, you can download the request to a computer that has management access to the FortiAnalyzer unit and then forward the request to a CA.

The certificate window also enables you to export certificates for authentication, importing and viewing.

Local certificates

The FortiAnalyzer has one default local certificate, *Fortinet_Local*. From this menu you can create, delete, import, view, and download local certificates.

The following information is displayed:

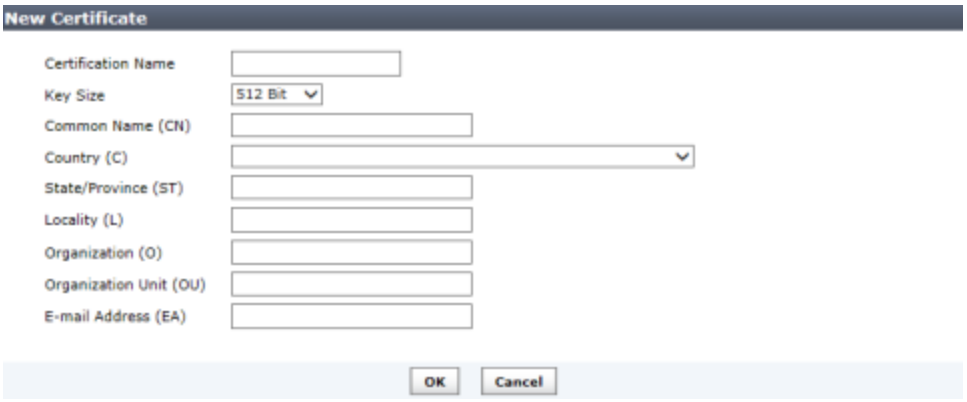
Certificate Name	Displays the certificate name.
Subject	Displays the certificate subject information.
Status	Displays the certificate status. Select *View Certificate Detail* to view additional certificate status information.

The following options are available:

Create New	Select to create a new certificate request.
Edit	Select the checkbox next to the certificate, right-click, and select Edit in the right-click menu to edit the entry. Alternatively, you can double-click the entry to open the New Certificate page.
Delete	Select the checkbox next to a certificate entry and select *Delete* to remove the certificate selected. Select *OK* in the confirmation dialog box to proceed with the delete action. Delete is also available in the right-click menu.
Import	Select to import a local certificate. Browse for the local certificate on the management computer and select *OK* to complete the import.
View Certificate Detail	Select the checkbox next to a certificate entry and select *View Certificate Detail* to view certificate details.
Download	Select the checkbox next to a certificate entry and select *Download* to download the certificate to your local computer.

To create a local certificate request:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select *Create New* in the toolbar. The *New Certificate* window opens.



3. Configure the following settings:

Certificate Name	The name of the certificate.
Key Size	Select the key size from the drop-down list. Select one of: *512 Bit*, *1024 Bit*, *1536 Bit*, or *2048 Bit*.
Common Name (CN)	Enter the common name of the certificate.
Country (C)	Select the country from the drop-down list.
State/Province (ST)	Enter the state or province.

Locality (L)	Enter the locality.
Organization (O)	Enter the organization for the certificate.
Organization Unit (OU)	Enter the organization unit.
E-mail Address (EA)	Enter the email address.

4. Select *OK* to save the setting. The request is sent and the status is listed as pending.

Only *Local Certificates* can be created. *CA Certificates* can only be imported

To view a local certificate:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select the certificates that you would like to see details about and select *View Certificate Detail* in the toolbar. The *Result* page opens.

The following information is displayed:

Certificate Name	The name of the certificate.
Issuer	The issuer of the certificate.
Subject	The subject of the certificate.
Valid From	The date from which the certificate is valid.
Valid To	The last day that the certificate is valid. The certificate should be renewed before this date.
Version	The certificate's version.
Serial Number	The serial number of the certificate.
Extension	The certificate extension information.

3. Select *OK* to return to the local certificates list.

CA certificates

The FortiAnalyzer has one default CA certificate, Fortinet_CA. In this sub-menu you can delete, import, and download CA certificates, and view certificate details.

To import a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select *Import* in the toolbar. The *Import* dialog box opens.
3. Select *Choose File*, browse to the location of the certificate, and select *OK*.

To view a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificates that you would like to see details about, then select *View Certificate Detail* in the toolbar. The *Result* page opens.

   The following information is displayed:

Certificate Name	The name of the certificate.
Issuer	The issuer of the certificate.
Subject	The subject of the certificate.
Valid From	The date from which the certificate is valid.
Valid To	The last day that the certificate is valid. The certificate should be renewed before this date.
Version	The certificate's version.
Serial Number	The serial number of the certificate.
Extension	The certificate extension information.

3. Select *OK* to return to the CA certificates list.

To download a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificates that you would like to download, select *Download* in the toolbar, and save the certificate to the desired location.

To delete a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificate or certificates that you would like to delete and select *Delete* in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the certificate.

Certificate revocation lists

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and Certificate Revocation List (CRL) from the issuing CA. When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiAnalyzer unit according to the procedures given below.

To import a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select *Import* in the toolbar. The *Import* dialog box opens.
3. Select *Browse*, browse to the location of the CRL, and select *OK*.

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL that you would like to see details about, then select *View Certificate Detail* in the toolbar. The *Result* page opens.
3. When you are finished viewing the CRL details, select *OK* to return to the CRL list.

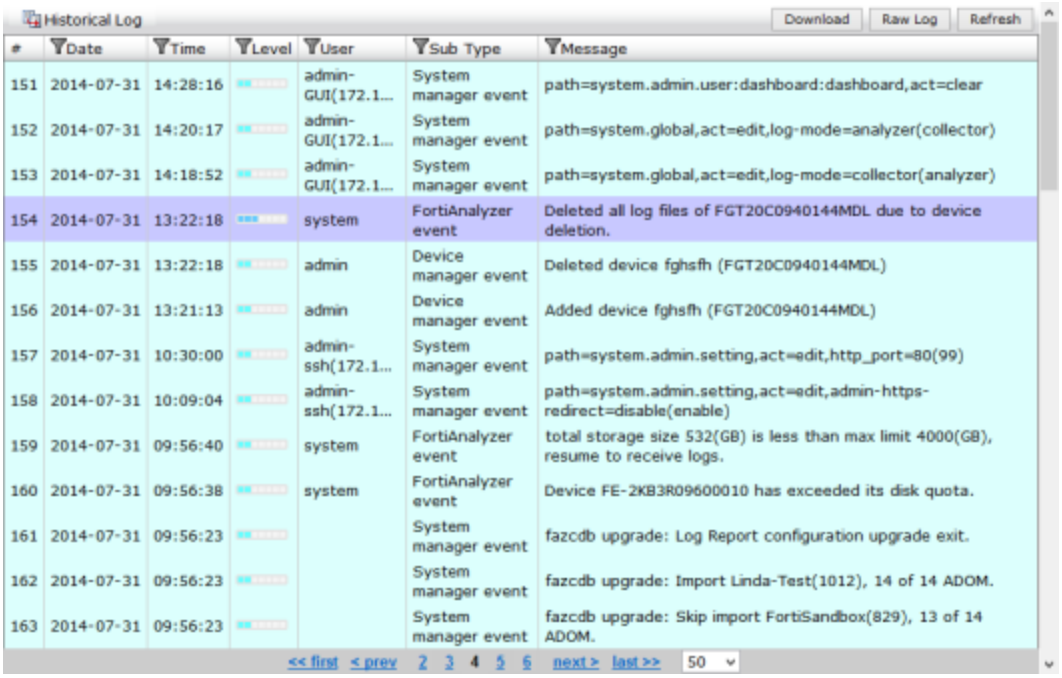
To delete a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL or CRLs that you would like to delete and select *Delete* in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the CRL.

Event log

The logs created by Fortinet are viewable within the GUI. You can use the *FortiAnalyzer Log Message Reference*, available in the Fortinet Document Library to interpret the messages. You can view log messages in the FortiAnalyzer GUI that are stored in memory or on the internal hard disk, and use the column filters to filter the event logs that are displayed.

Go to *System Settings* > *Event Log* to view the local log list.



The following information is displayed:

Type	Select the type from the drop down list. Select one of the following: *Event Log*, *FDS Upload Log*, or *FDS Download Log*. When selecting *FDS Upload Log*, select the device from the drop-down list, and select *Go* to browse logs. When selecting *FDS Download Log*, select the service (*FDS*, *FCT*) from the *Service* drop-down list, select the event type (*All Event*, *Push Update*, *Poll Update*, *Manual Update*) from the *Event* drop-down list, and *Go* to browse logs. This option is only available when viewing historical logs.
#	The log number.
Date	The date that the log file was generated. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter and specify the from and to date in the format YYYY-MM-DD. Select *Apply* to apply the filter, the filter. When the filter is enabled, the green filter enabled icon is displayed. You can also clear all filters.
Time	The time that the log file was generated. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter and specify the from and to time in the format HH:MM:SS. Select *Apply* to apply the filter. When the filter is enabled, the green filter enabled icon is displayed. You can also clear all filters.

Level	The log level. Select the filter icon to create a filter for this column. The following log levels are displayed: • Debug • Information • Notice • Warning • Error • Critical • Alert • Emergency Select the checkbox to enable this filter. Select a value for the field from the drop-down list, select the checkbox (NOT) if required, and select the level from the drop-down list. Select *Apply* to apply the filter. When the filter is enabled, the green filter enabled icon is displayed. You can also clear all filters.
User	User information. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter. Select a value for the field from the drop-down list, select the checkbox (NOT) if required, and enter the username in the text field. Select *Apply* to apply the filter. When the filter is enabled, the green filter enabled icon is displayed. You can also clear all filters.
Sub Type	Log sub-type information. Select the filter icon, to create a filter for this column. Select the checkbox to enable this filter, then select one or more of the event types. Select *Apply* to apply the filter. When the filter is enabled, the green filter enabled icon is displayed. You can also clear all filters. The available event types are: *System manager event*, *FG-FM protocol event*, *Device configuration event*, *Deployment manager event*, *Real-time monitor event*, *Log and report manager event*, *Firmware manager event*, *FortiGuard service event*, *FortiClient manager event*, *FortiMail manager event*, *Debug I/O log event*, *Device manager event*, *Web service event*, *FortiAnalyzer event*, *Log daemon event*, and *Device manager event*.
Message	Log message details. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter. Select a value for the field from the drop-down list, select the checkbox (NOT) if required, and enter a message in the text field. Select *Apply* to apply the filter. When the filter is enabled, the green filter enabled icon is displayed. You can also clear all filters.
Pagination	Use these page options to browse logs. You can select to display 50, 100, or 200 logs from the drop-down list.

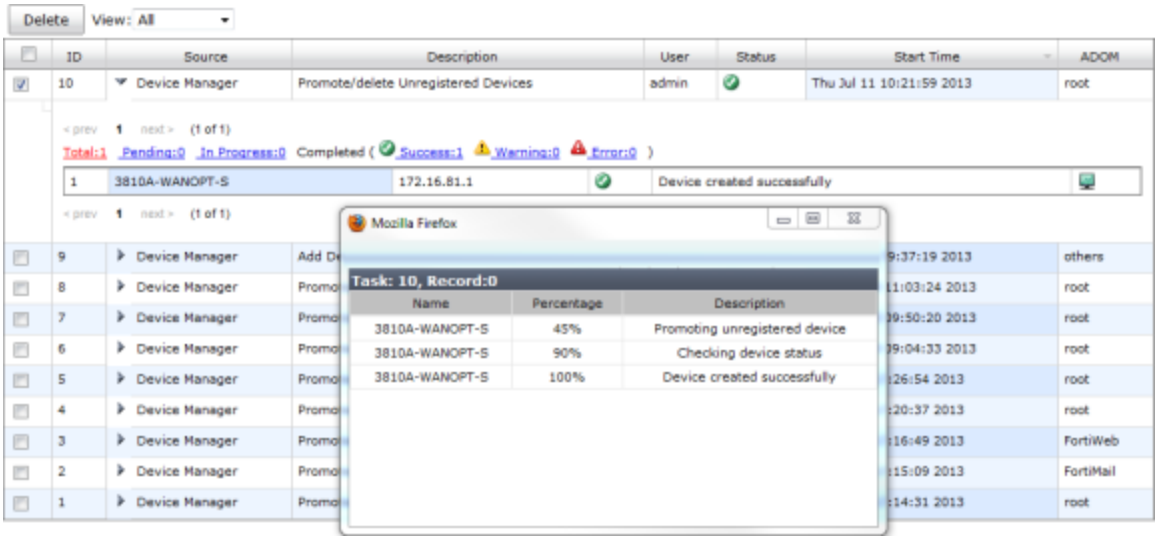
The following options are available in the toolbar:

Column Settings	Select to open the column settings dialog bog. You can edit which columns are displayed and the order in which they appear.
Historical Log	Select to view the historical log.
Download	Select to download the event log elog. You can download the file as a comma separated value (CSV) file or in a normal format. Select *OK* to save the file to your management computer.
Raw Log/Formatted Table	Select to display either raw logs for a formatted table.
Refresh	Select to refresh the information displayed in the log table.

Task monitor

Using the task monitor, you can view the status of the tasks that you have performed.

Go to *System Settings* > *Task Monitor*, then select a task category in the *View* field. Select the history icon for task details.



The following information is displayed:

ID	The identification number for a task.
Source	The platform from where the task is performed.
Expand Arrow	Select to display the specific actions taken under this task.
Description	The nature of the task.
User	The users who have performed the tasks.

Status	The status of the task (hover over the icon to view the description): • *All*: All types of tasks. • *Done*: Completed with success. • *Error*: Completed without success. • *Cancelled*: User cancelled the task. • *Cancelling*: User is cancelling the task. • *Aborted*: The FortiAnalyzer system stopped performing this task. • *Aborting*: The FortiAnalyzer system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column.
Start Time	The time that the task was performed.
ADOM	The ADOM associated with the task.
History	Select the history icon to view task details.

The following options are available in the toolbar:

Delete	Remove the selected task or tasks from the list.
Cancel Running Task(s)	Cancel the currently running task or tasks. This option is available when the selected view is *Running*.
View	Select which tasks to view from the drop-down list, based on their status. Select one of the following: *Running*, *Pending*, *Done*, *Error*, *Cancelling*, *Cancelled*, *Aborting*, *Aborted*, *Warning*, or *All*.

Advanced

The advanced tree menu enables you to configure SNMP, meta field data, and other settings. The following options are available:

SNMP	Select to configure FortiGate and FortiAnalyzer reporting through SNMP traps. See SNMP v1/v2c on page 105.
Mail Server	Select to configure mail server settings. See Mail server on page 109.
Syslog Server	Select to configure syslog server settings. See Syslog server on page 109.
Meta Fields	Select to configure meta-fields. See Meta fields on page 110.
Device Log Settings	Select to configure log settings and access and to view the task monitor. See Device log settings on page 111

File Management	Select to configure automatic deletion settings for file and reports. See File management on page 112.
Advanced settings	Select to configure ADOM mode, download the WSDL file, and configure the task list size. See Advanced settings on page 113.

SNMP v1/v2c

Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, such as the FortiAnalyzer SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is typically a computer running an application that can read the incoming trap and event messages from the agent and send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager, or host, to one or more FortiAnalyzer units.

By using an SNMP manager, you can access SNMP traps and data from any FortiAnalyzer interface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiAnalyzer unit it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiAnalyzer unit, or to query that unit.

You can configure the FortiAnalyzer unit to respond to traps and send alert messages to SNMP managers that were added to SNMP communities. When you are configuring SNMP, you need to first download and install both the FORTINET-CORE-MIB.mib and FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib files so that you can view these alerts in a readable format. The Fortinet MIB contains support for all Fortinet devices, and includes some generic SNMP traps; information responses and traps that FortiAnalyzer units send are a subset of the total number supported by the Fortinet proprietary MIB.

Your SNMP manager may already include standard and private MIBs in a compiled database which is all ready to use; however, you still need to download both the FORTINET-CORE-MIB.mib and FORTINET-FORTIANALYZER-MIB.mib files regardless.

FortiAnalyzer SNMP is read-only: SNMP v1 and v2 compliant SNMP managers have read-only access to FortiAnalyzer system information and can receive FortiAnalyzer traps. RFC support includes most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). FortiAnalyzer units also use object identifiers from the Fortinet proprietary MIB.

For more information about the MIBs and traps that are available for the FortiAnalyzer unit, see Appendix E - SNMP MIB Support on page 248.

SNMP traps alert you to events that happen, such as an a log disk being full or a virus being detected.

SNMP fields contain information about your FortiAnalyzer unit, such as percent CPU usage or the number of sessions. This information is useful to monitor the condition of the unit, both on an ongoing basis and to provide more information when a trap occurs.

Configuring the SNMP agent

The SNMP agent sends SNMP traps that originate on the FortiAnalyzer system to an external monitoring SNMP manager defined in one of the FortiAnalyzer SNMP communities. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiAnalyzer system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiAnalyzer system will

be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiAnalyzer system requires attention.

Go to *System Settings* > *Advanced* > *SNMP* to configure the SNMP agent.

The following information and options are available:

SNMP Agent	Select to enable the FortiAnalyzer SNMP agent. When this is enabled, it sends FortiAnalyzer SNMP traps.
Description	Type a description of this FortiAnalyzer system to help uniquely identify this unit.
Location	Type the location of this FortiAnalyzer system to help find it in the event it requires attention.
Contact	Type the contact information for the person in charge of this FortiAnalyzer system.
Communities	The list of SNMP communities added to the FortiAnalyzer configuration.
Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see Configuring an SNMP community on page 106.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
Enable	Select to enable or deselect to disable the SNMP community.
Delete	Select the delete icon to remove an SNMP community.
Edit	Select the edit icon to edit an SNMP community.

Configuring an SNMP community

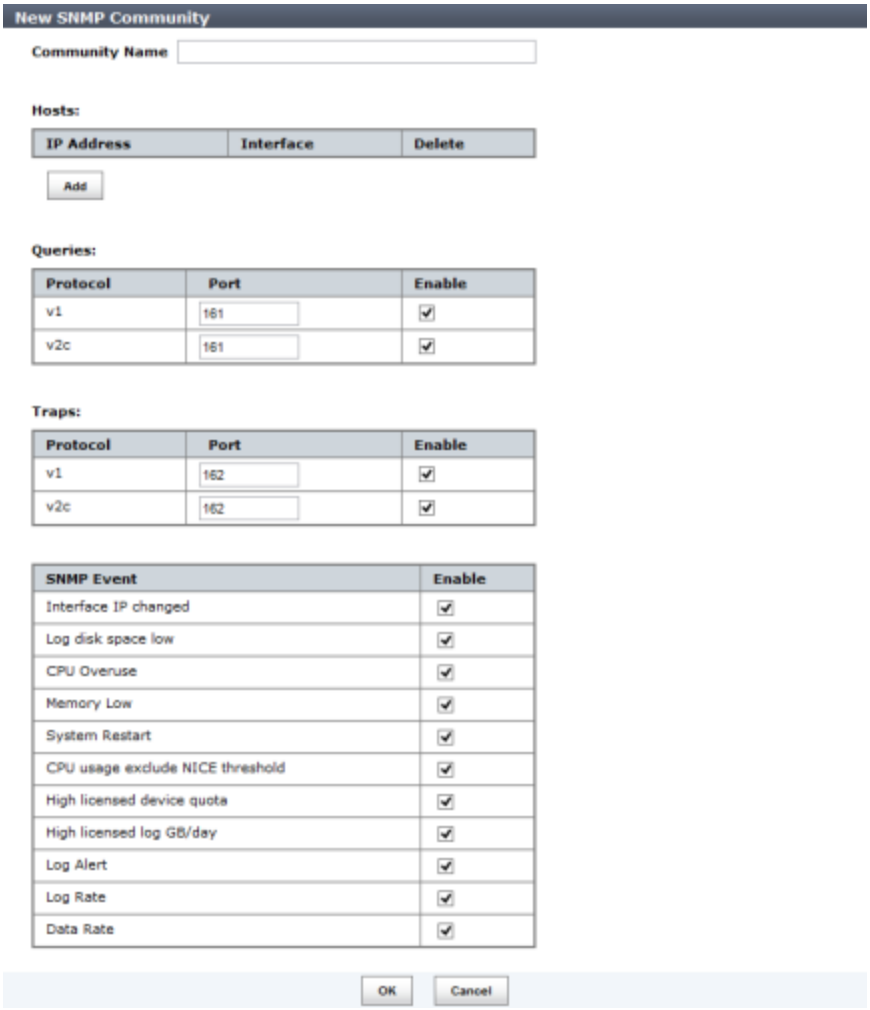
An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP community and a printer SNMP community.

You can add an SNMP community to define a destination IP address that can be selected as the recipient (SNMP manager) of FortiAnalyzer unit SNMP alerts. Defined SNMP communities are also granted permission to request FortiAnalyzer unit system information using SNMP traps.

Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiAnalyzer unit for a different set of events. You can also add the IP addresses of up to eight SNMP managers to each community.

To create a new SNMP community:

1. Go to *System Settings* > *Advanced* > *SNMP v1/v2c*.
2. Ensure that the *SNMP Agent* is enabled and, under *Communities*, select *Create New*. The *New SNMP Community* dialog box opens.



3. Configure the following settings:

Community Name	Type a name to identify the SNMP community. If you are editing an existing community, you will be unable to change the name.
Hosts	The list of hosts that can use the settings in this SNMP community to monitor the FortiAnalyzer system. Select *Add* to create a new entry that you can edit.

	IP Address	Type the IP address of an SNMP manager. By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.
	Interface	Select the name of the interface that connects to the network where this SNMP manager is located from the drop-down list. You need to do this if the SNMP manager is on the Internet or behind a router.
	Delete	Select the delete icon to remove this SNMP manager entry.
	Add	Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to eight SNMP manager entries for a single community.
Queries		Type the port number (161 by default) that the FortiAnalyzer system uses to send SNMPv1 and SNMPv2c queries to the FortiAnalyzer in this community. Enable queries for each SNMP version that the FortiAnalyzer system uses.
Traps		Type the Remote port number (162 by default) that the FortiAnalyzer system uses to send SNMPv1 and SNMPv2c traps to the FortiAnalyzer in this community. Enable traps for each SNMP version that the FortiAnalyzer system uses.
SNMP Event		Enable the events that will cause the FortiAnalyzer unit to send SNMP traps to the community. FortiAnalyzer SNMP events: • Interface IP changed • Log disk space low • CPU Overusage • Memory Low • System Restart • CPU usage exclude NICE threshold • RAID Event • This SNMP event is available for devices which support RAID. • High licensed device quota • High licensed log GB/day • Log Alert • Log Rate • Data Rate

4. Select *OK* to create the SNMP community.

To edit an SNMP community:

1. Go to *System Settings* > *Advanced* > *SNMP v1/v2c*.
2. In the *Action* column of the community you need to edit, select the edit icon. The *Edit SNMP Community* dialog box opens.
3. Edit the SNMP community settings as required and then select *OK*.

To delete an SNMP community:

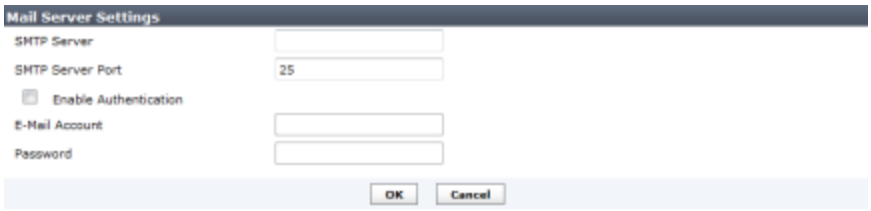
1. Go to *System Settings* > *Advanced* > *SNMP v1/v2c*.
2. In the *Action* column of the community you need to delete, select the delete icon.
3. Select *OK* in the confirmation dialog box to delete the SNMP community.

Mail server

Configure SMTP mail server settings for alerts, edit existing settings, or delete mail servers.

If an existing mail server is set in an *Event Handler* configuration, the delete icon is removed and the mail server entry cannot be deleted.

Select *Create New* in the toolbar to configure mail server settings.



Configure the following settings and then select *OK*:

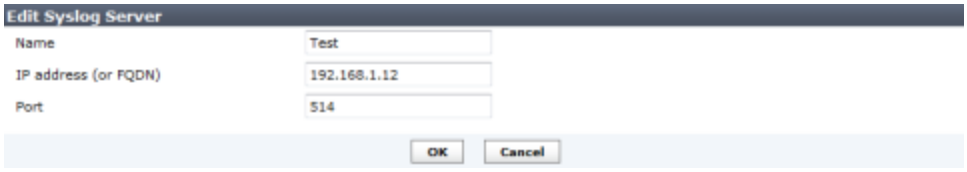
SMTP Server	Enter the SMTP server domain information, e.g. mail@company.com.
SMTP Server Port	Enter the SMTP server port number. The default port is 25.
Enable Authentication	Select to enable authentication.
Email Account	Enter an email account, e.g. admin@company.com.
Password	Enter the email account password.

Syslog server

Configure syslog server settings for alerts, edit existing settings, or delete syslog servers. Select *Create New* in the toolbar to add a new syslog server.

If an existing syslog server is set in an *Event Handler* configuration, the delete icon is removed and the syslog server entry cannot be deleted.

Select *Create New* to configure a new syslog server.



Configure the following settings and then select *OK*:

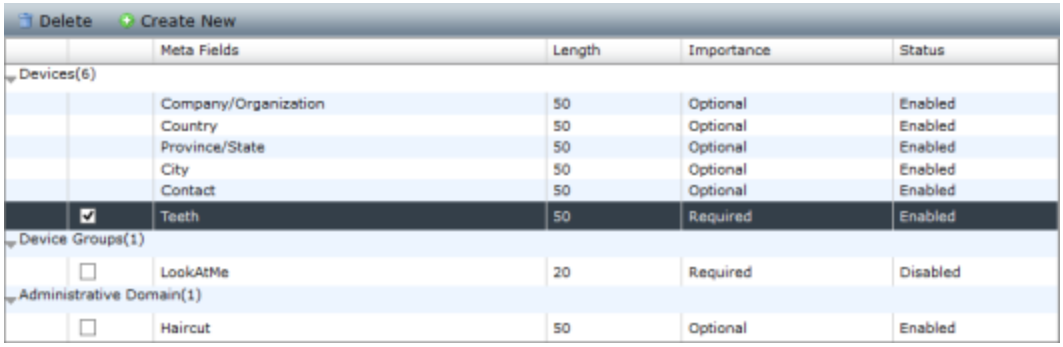
Name	Enter a name for the syslog server.
IP address (or FQDN)	Enter the IP address or FQDN of the syslog server.
Port	Enter the syslog server port number. The default port is 514.

Meta fields

Meta fields allow administrators to add extra information when configuring, adding, or maintaining FortiGate units. You can make the fields mandatory or optional, and set the length of the field.

With the fields set as mandatory, administrators must supply additional information when they create a new FortiGate object, such as an administrator account or firewall policy. Fields for this new information are added to the FortiGate unit dialog boxes in the locations where you create these objects. You can also provide fields for optional additional information.

Go to *System Settings* > *Advanced* > *Meta Fields* to configure meta fields.



The following information is displayed:

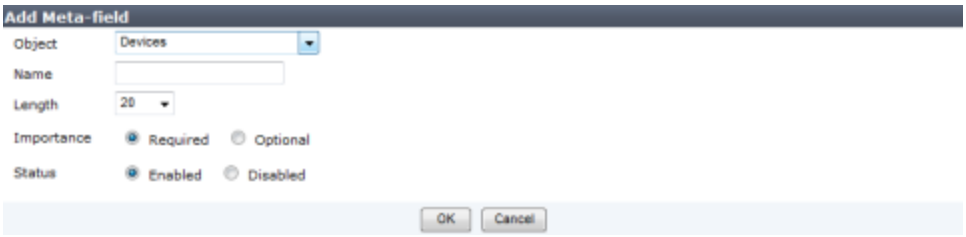
Meta Field	The name of this meta data field. Select the name to edit this field.
Length	The maximum length of this metadata field.
Importance	Indicates whether this field is required or optional.
Status	Indicates whether this field is enabled or disabled.

The following options are available in the toolbar:

Create New	Create a new meta data field for this object.
Delete	Delete the selected meta data field.

To create a new metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Select *Create New* in the toolbar. The *Add Meta-field* window opens.



3. Configure the following settings:

Object	The system object to which this metadata field applies. Select either *Devices*, *Device Groups*, or *Administrative Domains*.
Name	Enter the label to use for the field.
Length	Select the maximum number of characters allowed for the field from the drop-down list (*20*, *50*, or *255*).
Importance	Select *Required* to make the field compulsory, otherwise select *Optional.*
Status	Select *Disabled* to disable this field. The default selection is *Enabled*.

4. Select *OK* to create the new field.

To edit a metadata field:

1. From the meta field list, either double-click a meta filed, or right-click on a meta field then select *Edit*. The *Edit Meta-field* dialog box opens. Only the length, importance, and status of the meta field can be edited.
2. Edit the settings as required, then select *OK* to apply the changes.

To delete metadata fields:

1. From the meta field list, select the meta fields that you need to delete. The default meta fields cannot be deleted.
2. Select *Delete*, in the toolbar, then select *OK* in the confirmation box to delete the fields.

Device log settings

The device log settings menu allows you to configure event logging, log rollover, and upload options.

Go to *System Settings* > *Advanced* > *Device Log Settings* to configure device log settings.

Configure the following settings and select *Apply* to apply your changes:

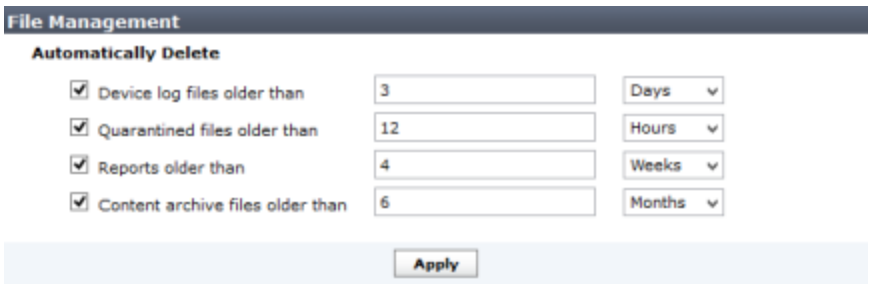
Rollover Options	
Roll log file when size exceeds	Enter the log file size, from 50 to 500 MB.

Roll log files at a regular time	Select to roll logs daily or weekly. When selecting daily, select the hour and minute value in the drop-down lists. When selecting weekly, select the day, hour, and minute value in the drop-down lists.
Enable log uploading	Select to upload logs and configure the following settings.
Upload Server Type	Select one of *FTP*, *SFTP*, or *SCP*.
Upload Server IP	Enter the IP address of the upload server.
Username	Select the username that will be used to connect to the upload server.
Password	Select the password that will be used to connect to the upload server.
Remote Directory	Select the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs* or daily at a specific hour.
Upload rolled files in gzipped format	Select to gzip the logs before uploading. This will result in smaller logs, and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiAnalyzer system after they have been uploaded to the Upload Server.

File management

FortiAnalyzer allows you to configure automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time.

To configure automatic deletion settings, go to *System Settings* > *Advanced* > *File Management*.



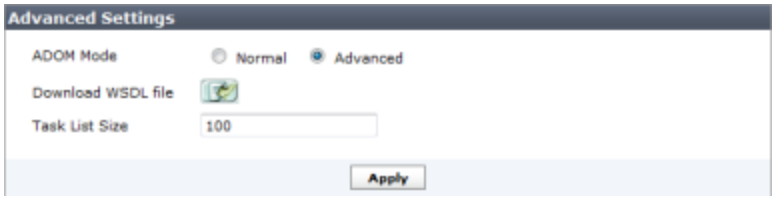
Configure the following settings:

Device log files older than	Select to enable this feature, enter a value in the text field, then select the time period from the drop-down list (*Hours*, *Days*, *Weeks*, or *Months*)

Quarantined files older than	Select to enable this feature, enter a value in the text field, and select the time period from the drop-down list.
Reports older than	Select to enable this feature, enter a value in the text field, and select the time period from the drop-down list.
Content archive files older than	Select to enable this feature, enter a value in the text field, and select the time period from the drop-down list.

Advanced settings

To view and configure advanced settings options, go to the *System Settings* > *Advanced* > *Advanced Settings* page.



Advanced ADOM mode will allow users to assign VDOMs from a single device to different ADOMs, but will result in a reduced operation mode and more complicated management scenarios. It is recommended for advanced users only.

Configure the following settings and then select *Apply*:

ADOM Mode	Select either *Normal* or *Advanced*. In normal mode, you can only add FortiGate devices to an ADOM. In advanced mode, you can add FortiGate devices and/or their VDOMs to an ADOM.
Download WSDL file	Select to download the FortiAnalyzer unit's WSDL file. Web services is a standards-based, platform independent, access method for other hardware and software application programming interfaces (APIs). The file itself defines the format of commands the FortiAnalyzer unit will accept, as well as the response to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiAnalyzer unit and operate it or retrieve information just as an admin user would from the GUI or CLI.
Task List Size	Set a limit on the size of the task list.

FortiView

The *FortiView* tab allows you to access both FortiView drill down and Log view menus. FortiView in FortiAnalyzer collects data from FortiView in FortiGate. In order for information to appear in the FortiView dashboards in FortiGate, disk logging must be selected for the FortiGate unit.

When rebuilding the SQL database, FortiView will not be available until after the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

FortiView

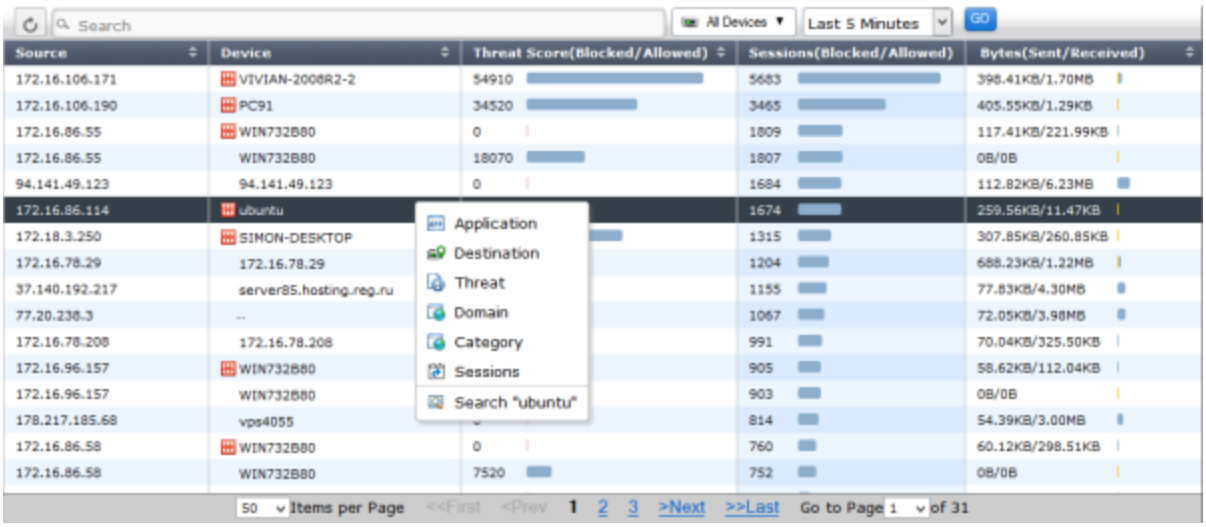
Use FortiView to drill down real-time and historical traffic from log devices by sources, applications, destinations, web sites, threats, cloud applications. Each dashboard can be filtered by a variety of attributes, as well as by device and time period. These attributes can be selected using the right-click context menu. Results can also be filtered using the various columns.

The following summary views are available:

- Top Sources
- Top Applications
- Top Destinations
- Top Web Sites
- Top Threats
- Top Cloud Applications

Top Sources

The *Top Sources* dashboard displays information about the sources of traffic on your FortiGate unit. You can drill down the displayed information, select the device and time period, and apply search filters.



The following information is displayed:

Source	Displays the source IP address and/or user name, if applicable. Select the column header to sort entries by source. You can apply a search filter to the source (`srcip`) column.
Device	Displays the device IP address or FQDN. Select the column header to sort entries by device. You can apply a search filter to the device (`dev_src`) column.
Threat Weight	Displays the threat weight value. Select the column header to sort entries by threat weight.
Sessions	Displays the number of sessions. Select the column header to sort entries by sessions.
Bandwidth (Sent/Received)	Displays the bandwidth value for sent and received packets. Select the column header to sort entries by bandwidth.Custom

The following options are available:

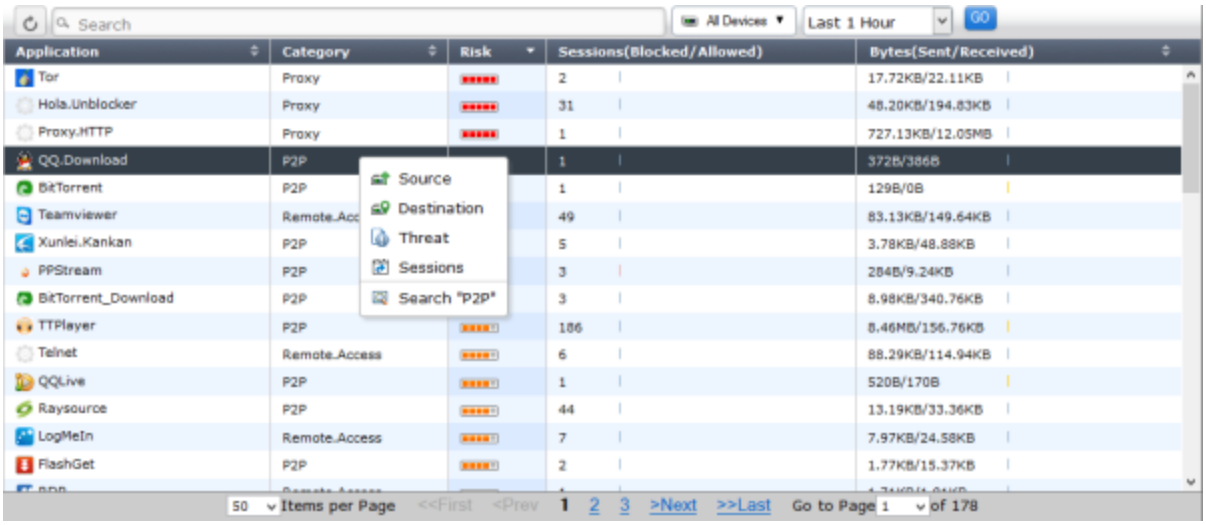
Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter for user (`user`), source IP (`srcip`), source device (`dev_src`), source interface (`srcintf`), destination interface (`dstintf`), policy ID (`policyid`), security action (utmaction) or virtual domain (`vd`). Select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter. Select the clear icon to remove the search filter.
Devices	Select the devices from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.

Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Application	Select to drill down by application to view application related information including the application, number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the application (`app`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat weight, and number of sessions. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threat-type`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Domain	Select to drill down by domain to view domain related information including domain, category, browsing time, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. Select the *GO* button to apply the search filter.Select the return icon to return to the *Top Sources* page.

Category	Select to drill down by category to view category related information including category, browsing time, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Search	Add a search filter by source IP (`srcip`) or source device (`dev_src`). Select the GO button to apply the filter. Select the clear icon to remove the search filter.

Top Applications

The *Top Applications* dashboard shows information about the applications being used on your network, including the application name, category, and risk level. You can drill down the displayed information, select the device and time period, and apply search filters.



The following information is displayed:

Application	Displays the application name and service. Select the column header to sort entries by application. You can apply a search filter to the application (`app`) column.

Category	Displays the application category. Select the column header to sort entries by category. You can apply a search filter to the category (`appcat`) column.
Risk	Displays the application risk level. Hover the mouse cursor over the entry in the column for additional information. Select the column header to sort entries by risk. Risk uses a new 5-point risk rating. The rating system is as follows: • *Critical*: Applications that are used to conceal activity to evade detection. • *High*: Applications that can cause data leakage, are prone to vulnerabilities, or downloading malware. • *Medium*: Applications that can be misused. • *Elevated*: Applications that are used for personal communications or can lower productivity. • *Low*: Business related applications or other harmless applications.
Sessions	Displays the number of sessions. Select the column header to sort entries by sessions.
Bandwidth (Sent/Received)	Displays the bandwidth value for sent and received packets. Select the column header to sort entries by bandwidth.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter for user (`user`), source IP (`srcip`), source device (`dev_src`), source interface (`srcintf`), destination interface (`dstintf`), policy ID (`policyid`), security action (`utmaction`) or virtual domain (`vd`). Select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter. Select the clear icon to remove the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.

Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Source	Select to drill down by source to view source related information including the source IP address, device MAC address or FQDN, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.
Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.
Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat weight, and number of sessions. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threat-type`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.
Search	Add a search filter by application or category. Select the GO button to apply the filter. Select the clear icon to remove the search filter.

Top Destinations

The *Top Destinations* dashboard shows information about the destination IP addresses of traffic on your FortiGate unit, as well as the application used. You can drill down the displayed information, select the device

and time period, and apply search filters.

The following information is displayed:

Destination	Displays the destination IP address and geographic region. A flag icon is displayed to the left of the IP address. Select the column header to sort entries by destination. You can apply a search filter to the destination (`dstip`) column.
Application	Displays the application port and service. When the information displayed exceeds the column width, hover the mouse cursor over the entry in the column for a full list. Select the column header to sort entries by application. You can apply a search filter to the application (`app`) column.
Sessions	Displays the number of sessions. Select the column header to sort entries by sessions.
Bandwidth (Sent/Received)	Displays the bandwidth value for sent and received packets. Select the column header to sort entries by bandwidth.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter by destination IP, source interface (`srcintf`), destination interface (`dstintf`), policy ID (`policyid`), security action (`utmaction`), or virtual domain (`vd`). Select the GO button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter. Select the clear icon to remove the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	

Application	Select to drill down by application to view application related information including the service and port, number of sessions (blocked/allowed), and bandwidth (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the application (`app`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.
Source	Select to drill down by source to view source related information including the source IP address, device MAC address or FQDN, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.
Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat weight, and number of sessions. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threattype`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Search	Add a search filter by destination IP. Select the GO button to apply the filter. Select the clear icon to remove the search filter.

Top Web Sites

The *Top Web Sites* dashboard lists the top allowed and top blocked web sites. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Domain	Displays the domain name. Select the column header to sort entries by domain. You can apply a search filter to the domain (`domain`) column. This column is only shown when *Domain* is selected in the domain/category drop-down list.
Category	Displays the web site category. When the information displayed exceeds the column width, hover the mouse cursor over the entry in the column for a full list. Select the column header to sort entries by category.
Browsing Time	Displays the web site browsing time. Select the column header to sort entries by browsing time.
Threat Weight	Displays the web site threat weight value. Select the column header to sort entries by threat weight.
Sessions	Displays the number of sessions blocked and allowed. Select the column header to sort entries by sessions.
Bandwidth (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bandwidth.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter by destination IP, source interface (`srcintf`), destination interface (`dstintf`), policy ID (`policyid`), security action (`utmaction`), or virtual domain (`vd`). Select the GO button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter. Select the clear icon to remove the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Domain/Category	Select to view information based on either the domain or the category.
Go	Select the *GO* button to apply the filter.

Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Source	Select to drill down by source to view source related information including the source IP address, device IP address or FQDN, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Web Sites* page.
Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Web Sites* page.
Category	Select to drill down by category to view category related information including category, browsing time, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Web Sites* page.
Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat weight (blocked/allowed), and number of incidents (blocked/allowed). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threattype`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.

Search	Add a search filter by domain (`domain`) or category (`catdesc`). Select the GO button to apply the filter. Select the clear icon to remove the search filter.

Top Threats

The *Top Threats* dashboard lists the top users involved in incidents, as well as information on the top threats to your network. You can drill down the displayed information, select the device and time period, and apply search filters.

The following incidents are considered threats:

- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus.

The following information is displayed:

Threat	Displays the threat type. Select the column header to sort entries by threat. You can apply a search filter to the threat (`threat`) column.
Category	Displays the threat category. Select the column header to sort entries by category. You can apply a search filter to the category (`threattype`) column.
Threat Level	Displays the threat level. Select the column header to sort entries by threat level.
Threat Weight	Displays the threat weight value. Select the column header to sort entries by threat weight.
Incidents	Displays the number of incidents for this threat type. Select the column header to sort entries by incidents.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter by destination IP, source interface (`srcintf`), destination interface (`dstintf`), policy ID (`policyid`), security action (`utmaction`), or virtual domain (`vd`). Select the GO button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter. Select the clear icon to remove the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.

Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Source	Select to drill down by source to view source related information including the source IP address, device MAC address or FQDN, threat weight, number of sessions, and bandwidth (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Threats* page.
Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat weight value, number of sessions, and bandwidth (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Threats* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Threats* page.
Search	Add a search filter by threat (`threat`) or category (`threattype`). Select the GO button to apply the filter. Select the clear icon to remove the search filter.

Top Cloud Applications

The *Top Cloud Applications* dashboard displays information about the cloud application traffic on your FortiGate unit. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Application	Displays the application name. Select the column header to sort entries by application. You can apply a search filter to the application (`app`) column.
User	Displays the user name. Select the column header to sort entries by user. This column is only shown when *Cloud Users* is selected in the applications/users drop-down list.
Category	Displays the application category. Select the column header to sort entries by category. You can apply a search filter to the category (`appcat`) column. This column is only shown when *Cloud Applications* is selected in the applications/users drop-down list.
Risk	Displays the application risk level. Hover the mouse cursor over the entry in the column for additional information. Select the column header to sort entries by risk. Risk uses a new 5-point risk rating. The rating system is as follows: • *Critical*: Applications that are used to conceal activity to evade detection. • *High*: Applications that can cause data leakage, are prone to vulnerabilities, or downloading malware. • *Medium*: Applications that can be misused. • *Elevated*: Applications that are used for personal communications or can lower productivity. • *Low*: Business related applications or other harmless applications. This column is only shown when *Cloud Applications* is selected in the applications/users drop-down list.
Login IDs	Displays the number of login IDs associated with the application. Select the column header to sort entries by login ID. This column is only shown when *Cloud Applications* is selected in the applications/users drop-down list.
Sessions	Displays the number of sessions associated with the application. Select the column header to sort entries by category.
File (Up/Down)	Displays the number of files uploaded and downloaded. Hover the mouse cursor over the entry in the column for additional information. Select the column header to sort entries by file.
Videos Played	Displays the number of videos played using the application. Select the column header to sort entries by videos played.

Bandwidth (Sent/Received)	Displays the bandwidth value for sent and received packets. Select the column header to sort entries by bandwidth. Select the column header to sort entries by category.

The following options are available:

Search	Click the search field to add a search filter by application (`app`), source interface (`srcintf`), destination interface (`dstintf`), policy ID (`policyid`), security action (`utmaction`), or virtual domain (`vd`). Select the GO button to apply the search filter. Alternatively, you can right-click the column entry to dd the search filter. Select the clear icon to remove the search filter.
Devices	Select the device from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Cloud Applications / Cloud Users	Select to view information based on either applications or users.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Cloud Users / Cloud Applications	Select to drill down by cloud users to view user related information including IP address, source IP address, number of files uploaded and downloaded, number of videos plays, number of sessions, and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the user (`clouduser`) and source (`source`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.

Files	Select to drill down by files to view file related information including the user email address, source IP address, file name, and file size. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the user (`clouduser`) and source (`srcip`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.
Videos	Select to drill down by videos to view video related information including the user email address, source IP address, file name, and file size. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the user (`clouduser`) and source (`srcip`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.
Sessions	Select to drill down by sessions to view session related information including the date and time, source/device IP address, destination IP address, service, number of packets sent and received, user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), and application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.
Search	Add a search filter by cloud application (`app`), category (`appcat`), or cloud user (`clouduser`). Select the GO button to apply the filter. Select the clear icon to remove the search filter.

Log view

Logging and reporting can help you determine what is happening on your network, as well as informing you of certain network activity, such as the detection of a virus, or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information gathering, as well as displaying the activity that is happening on the network.

Your FortiAnalyzer device collects logs from managed FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiSandbox, FortiWeb, FortiClient, and syslog servers.

Device Type	Log Type
FortiGate	• Traffic • Event: Endpoint, HA, System, Router, VPN, User, WAN Opt. & Cache, and Wireless • Security: Vulnerability Scan, AntiVirus, Web Filter, Application Control, Intrusion Prevention, Email Filter, Data Leak Prevention • FortiClient • VoIP Content logs are also collected for FortiOS 4.3 devices.
FortiCarrier	Traffic, Event
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiClient	Traffic , Event
FortiMail	History, Event, Antivirus, Email Filter
FortiManager	Event
FortiSandbox	Malware, Network Alerts
FortiWeb	Event, Intrusion Prevention, Traffic
Syslog	Generic

Traffic logs record the traffic that is flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through the unit, this type of logging is also referred to as firewall policy logging. Firewall policies control all traffic that attempts to pass through the FortiGate unit, between FortiGate interfaces, zones and VLAN sub-interfaces.

The event log records administration management as well as Fortinet device system activity, such as when a configuration has changed, or admin login or HA events occur. Event logs are important because they record Fortinet device system activity, which provides valuable information about how your Fortinet unit is performing. The FortiGate event logs includes *System*, *Router*, *VPN*, and *User* menu objects to provide you with more granularity when viewing and searching log data.

Security logs (FortiGate) record all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, vulnerability scan, and VoIP activity on your managed devices.

The logs displayed on your FortiAnalyzer are dependent on the device type logging to it and the features enabled. FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox, FortiClient and Syslog logging is supported. ADOMs must be enabled to support non-FortiGate logging.

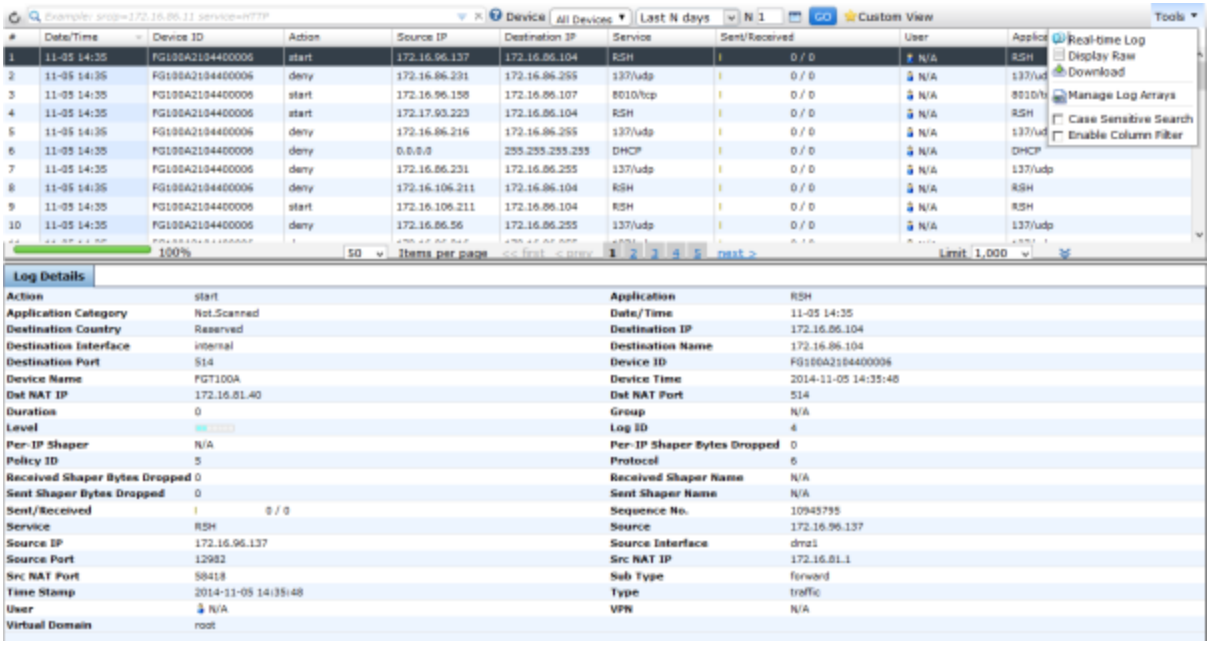
For more information on logging see the *Logging and Reporting for FortiOS Handbook* in the *Fortinet Document Library*.

The *Log View* menu displays log messages for connected devices. You can also view, import, and export log files that are stored for a given device, and browse logs for all devices.

When rebuilding the SQL database, Log View will not be available until after the rebuild is completed. Although you can view older logs, new logs will not be inserted into the database until after the rebuild is completed. Select the *Show Progress* link in the message to voew the status of the SQL rebuild.

Viewing log messages

To view log messages, select the *FortiView* tab, select *Log View* in the left tree menu, then browse to the ADOM whose logs you would like to view in the tree menu. You can view the traffic log, event log, or security log information per device or per log array. FortiMail and FortiWeb logs are found in their respective default ADOMs. For more information on FortiGate raw logs, see the *FortiGate Log Message Reference* in the *Fortinet Document Library*. For more information on other device raw logs, see the *Log Message Reference* for the platform type.



This page displays the following information and options:

Refresh	Select the icon to refresh the log view. This option is only available when viewing historical logs.
Search	Enter a search term to search the log messages. See To perform a text search: on page 136. You can also right-click an entry in one of the columns and select to add a search filter. Select *GO* in the toolbar to apply the filter. Not all columns support the search feature.

Latest Search	Select the icon to repeat previous searches, select favorite searches, or quickly add filters to your search. The filters available will vary based on device and log type.
Clear Search	Select the icon to clear search filters.
Help	Hover your mouse over the help icon, for example search syntax. See Examples on page 137.
Device	Select the device or log array in the drop-down list. Select *Manage Log Arrays* in the *Tools* menu to create, edit, or delete log arrays.
Time Period	Select a time period from the drop-down list. Options include: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, or *Custom*. See To customize the time period: on page 136. This option is only available when viewing historical logs.
GO	Select the icon to apply the time period and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
Custom View	Select to create a new custom view. You can select to create multiple custom views in log view. Each custom view can display a select device or log array with specific filters and time period. See To create a new custom view: on page 135. Custom views are displayed under the *Custom View* menu. This option is only available when viewing historical logs.
Pause | Resume	Pause or resume real-time log display. These two options are only available when viewing real-time logs.
Tools	The tools button provides options for changing the manner in which the logs are displayed, and search and column options. You can manage log arrays and it also provides an option for downloading logs, see Download log messages on page 137.
Real-time Log **Historical Log**	Select to change view from *Real-time Log* to *Historical Log*.
Display Raw	Select to change view from formatted display to raw log display.
Download	Select to download logs. A download dialog box is displayed. Select the log file format, compress with gzip, the pages to include and select *Apply* to save the log file to the management computer. This option is only available when viewing historical logs in formatted display.
Manage Log Arrays	Select to create new, edit, and delete log arrays. Once you have created a log array, you can select the log array in the *Device* drop-down menu in the *Log View* toolbar. In FortiAnalyzer 5.0.7 and later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.

	Case Sensitive Search	Select to enable case sensitive search.
	Enable Column Filter	Select to enable column filters.
	Display Log Details	Select to display the log details window.
Logs		The columns and information shown in the log message list will vary depending on the selected log type, the device type, and the view settings. Right-click on various columns to add search filters to refine the logs displayed. When a search filter is applied, the value is highlighted in the table and log details.
Log Details		Detailed information on the log message selected in the log message list. The item is not available when viewing raw logs. See Log details on page 138 for more information. *Log Details* are only displayed when enabled in the *Tools* menu.
Status Bar		Displays the log view status as a percentage.
Pagination		Adjust the number of logs that are listed per page and browse through the pages.
Limit		Select the maximum number of log entries to be displayed from the drop-down list. Options include: *1000*, *5000*, *10000*, *50000*, or *All*.
Archive		Information about archived logs, when they are available. The item is not available when viewing raw logs, or when the selected log message has no archived logs. When an archive is available, the archive icon is displayed. See Archive on page 139 for more information. This option is only available when viewing historical logs in formatted display and when an archive is available.

Customizing the log view

The log message list can show raw or formatted, real time or historical logs. The columns in the log message list can be customized to show only relevant information in your preferred order.

Log display

By default, historical formatted logs are shown in the log message list. You can change the view to show raw logs and both raw and formatted real time logs.

To view real time logs, in the log message list, select *Tools*, then select *Real-time Log* from the drop-down menu. To return to the historical log view, select *Tools*, then select *Historical Log* from the drop-down menu.

To view raw logs, in the log message list, select *View*, then select *Display Raw* from the drop-down menu. To return to the formatted log view, select *Tools*, then select *Display Formatted* from the drop-down menu.

This page displays the following information and options:

Refresh	Select to refresh the log view. This option is only available when viewing historical logs.
Search	Enter a search term to search the log messages. See To perform a text search: on page 136. You can also right-click an entry in one of the columns and select to add a search filter. Select *GO* in the toolbar to apply the filter. Not all columns support the search feature.
Latest Search	Select the icon to repeat previous searches, select favorite searches, or quickly add filters to your search. The filters available will vary based on device and log type.
Clear Search	Select the icon to clear search filters.
Help	Hover your mouse over the help icon, for example search syntax. See Examples on page 137.
Device	Select the device or log array in the drop-down list. Select *Manage Log Arrays* in the *Tools* menu to create, edit, or delete log arrays.
Time Period	Select a time period from the drop-down list. Options include: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, or *Custom*. See To customize the time period: on page 136. This option is only available when viewing historical logs.
GO	Select to apply the time period and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
Create Custom View	Select to create a new custom view. You can select to create multiple custom views in log view. Each custom view can display a select device or log array with specific filters and time period. See To create a new custom view: on page 135. This option is only available when viewing historical logs.
Pause | Resume	Pause or resume real-time log display. These two options are only available when viewing real-time logs.
Tools	The tools button provides options for changing the manner in which the logs are displayed, and search options. You can manage log arrays and it also provides an option for downloading logs, see Download log messages on page 137.
Real-time Log **Historical Log**	Select to change view from *Real-time Log* to *Historical Log*.
Display Formatted	Select to change view from raw log display to formatted log display.

	Download	Select to download logs. A download dialog box is displayed. Select the log file format, compress with gzip, the pages to include and select *Apply* to save the log file to the management computer. This option is only available when viewing historical logs in formatted display.
	Manage Log Arrays	Select to create new, edit, and delete log arrays. Once you have created a log array, you can select the log array in the *Device* drop-down menu in the *Log View* toolbar.
	Case Sensitive Search	Select to enable case sensitive search.
Detailed Information		Detailed information on the log message selected in the log message list. The item is not available when viewing raw logs.
Status Bar		Displays the log view status as a percentage.
Pagination		Adjust the number of logs that are listed per page and browse through the pages.
Limit		Select the maximum number of log entries to be displayed from the drop-down list. Options include: *1000*, *5000*, *10000*, *50000*, or *All*.

The selected log view will affect the other options that are available in the *View* drop-down menu. Real-time logs cannot be downloaded, and raw logs to not have the option to customize the columns.

Columns

The columns displayed in the log message list can be customized and reordered as needed. Filters can also be applied to the data in a column.

To customize the displayed columns:

1. In the log message list, right-click on a column heading. The *Column Settings* pop-up menu opens.
2. Select which columns to hide or display:
   - To add a column to the page, in the *Available Fields* area, select the columns you want to display, then select the right arrow to move them to the *Show fields in this order* area.
   - To remove a column from the page, in the *Show fields in this order* area, select the columns you want to hide, then select the left arrow to move them to the *Available Fields* area.
   - To return all columns to their default view, select *Default*.

The available column settings will vary based on the device and log type selected.

3. Adjust the order of the displayed columns:
   a. In the *Show fields in this order* area, select a column name.
   b. Select the up or down arrow to move the column up or down (left or right, respectively, in the log message

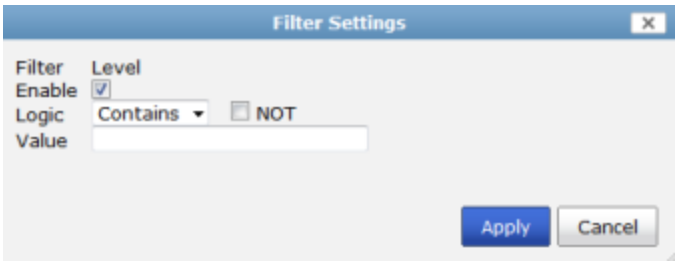
list).

4. Select *Apply* to apply your changes.

To filter column data:

1. In the log message list, select *View*, then select *Enable Column Filter* from the drop-down menu to enable column filters.
2. In the heading of the column you need to filter, select the filter icon. The filter icon will only be shown on columns that can filtered.

   The *Filter Settings* dialog box opens.



3. Enable the filter, then enter the required information to filter the selected column. The filter settings will vary based on the selected column.
4. Select *Apply* to apply the filter to the data.

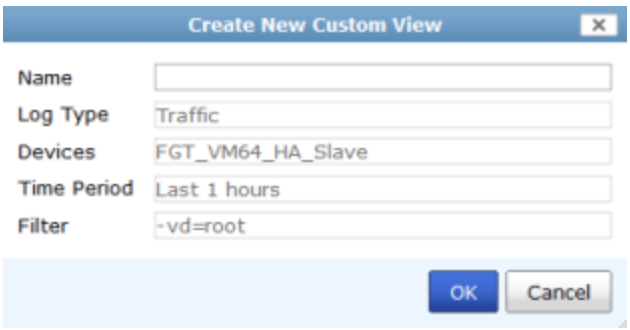
   The column's filter icon will turn green when the filter is enabled, Downloading the current view will only download the log messages that meet the current filter criteria.

Custom views

Select *Create Custom View* in the toolbar to create a new custom log view. Use *Custom View* to save a custom search, device selection, and time period so that you can select this view at any time to view results without having to re-select these criteria. Custom views are listed under the *Custom View* menu and allow you to quickly view log data based on specific time and content filters without having to re-configure filters.

To create a new custom view:

1. In the *Log View* pane, select an ADOM, and select the log type.
2. Add a custom search term, select a device or devices, select a time period, limit the number of logs to display as needed, then select *Go*.
3. Select Custom View in the toolbar. The *Create New Custom View* dialog box is displayed.



4. Enter a name for the new custom view. All other fields are read-only. The new custom view is saved to the Custom View folder in the ADOM.

To edit a custom view:

1. In the *Log View* pane, select an ADOM, and select the *Custom View* folder in the tree menu.
2. Select the custom view you would like to edit.
3. Edit the custom search, devices, time period, limit the number of logs to display, and select *GO*.
4. Right-click the name of the custom view and select *Save* to save your changes.

To rename a custom view:

1. In the *Log View* pane, select an ADOM, and select the *Custom View* folder.
2. Right-click the name of the custom view and select *Rename* in the menu. The *Rename Custom View* dialog box opens.
3. Edit the name and select *OK* to save your changes.

To delete a custom view:

1. In the *Log View* pane, select an ADOM, and select the *Custom View* folder.
2. Right-click the name of the custom view and select *Delete* in the menu.
3. Select *OK* in the confirmation dialog box to delete the view.

Searching log messages

Log messages can be searched based on a text string and/or time period. Recent searches can be quickly repeated, a time period can be specified or customized, and the number of displayed logs can be limited. A text string search can be case sensitive or not as required.

To perform a text search:

1. In the log message list, select *View*, then either select or deselect *Case Sensitive Search* from the drop-down menu to enable or disable case sensitivity in the search string.
2. In the log message list, enter a text string in the search field in the following ways:
   - Manually type in the text that you are searching for. Wildcard characters are accepted.
   - Right-click on the element in the list that you would like to add to the search and select to search for strings that either match or don't match that value.
   - Select a previous search or default filter, using the history icon. The available filters will vary depending on the selected log type and displayed columns.
   - Paste a saved search into the search field.
3. Select *GO* to search the log message list.

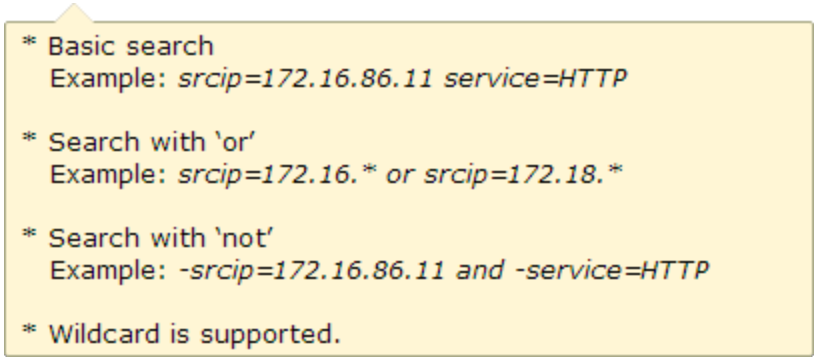
To customize the time period:

1. In the log message list, open the time period drop-down menu, and select *Custom...*. The *Custom Timeframe* dialog box opens.
2. Specify the desired time period using the *From* and *To* fields, or select *Any Time* to remove any time period from the displayed data.

3. Select *Apply* to create the custom time period. A calendar icon will be shown next to the time period drop-down list. Select it to adjust the custom time period settings.
4. Select *GO* to apply your settings to the log message list.

Examples

To view example text search strings, hover your cursor over the help icon.



The first example will search for log messages with a source IP address of 172.16.86.11 and a service of HTTP. Because it is not specified, the and operator is assumed, meaning that both conditions must be met for the log message to be included in the search results.

The second example will search for any log messages with source IP addresses that start with either 172.16 or 172.18. Notice the use of the * wildcard. The use of the *or* operator means that either condition can be met for the log message to be included in the search results.

The third example will search for any log message that do not have a source IP address of 172.16.86.11 and a service of HTTP. The use of the *and* operator means that both conditions must be met for the log message to be excluded from the search results.

Download log messages

Log messages can be downloaded to the management computer as a text or CSV file. Real time logs cannot be downloaded.

To download log messages:

1. In the log message list, select *View*, then select *Download*. The *Download* dialog box opens.
2. Select a log format from the drop down list, either *Text* or *CSV*.
3. Select *Compress with gzip* to compress the downloaded file.
4. Select *Current Page* to download only the current log message page, or *All Pages* to download all of the pages in the log message list.
5. Select *Apply* to download the log messages to the management computer.

Log arrays

Log Array has been relocated to *Log View* in the *FortiView* module from the *Device Manager* module. Upon upgrading to FortiAnalyzer 5.0.9 and later, all previously configured log arrays will be imported. In FortiAnalyzer 5.0.6 and earlier, when creating a Log Array with both devices and VDOMs, you need to select each device and

VDOM to add it to the Log Array. In FortiAnalyzer 5.0.7 and later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.

To create a new log array:

1. In the *Log View* pane, select the *Tools* button, and select *Manage Log Arrays*. The *Manage Log Arrays* dialog box opens.
2. Select *Create New* in the dialog box toolbar. The *Create New Log Array* dialog box opens.
3. Enter the following:

Name	Enter a unique name for the log array.
Comments	Enter optional comments for the log array.
Devices	Select the add icon and select devices and VDOMs to add to the log array. Select *OK* in the device selection window.

4. Select *OK* to create the new log array.
5. Select the close icon to close the *Manage Log Arrays* dialog box.

To edit a log array:

1. In the *Log View* pane, select *Tools*, and select *Manage Log Arrays*. The *Manage Log Arrays* dialog box is displayed.
2. Select a log array entry and select *Edit* in the toolbar. The *Edit Log Array* dialog box is displayed.
3. Edit the log array name, comments, and devices as needed.
4. Select *OK* to save the log array.
5. Select the close icon to close the *Manage Log Arrays* dialog box.

To delete a log array:

1. In the *Log View* pane, select *Tools*, and select *Manage Log Arrays*. The *Manage Log Arrays* dialog box is displayed.
2. Select the log array entry and select *Delete* in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the log array.
4. Select the close icon to close the *Manage Log Arrays* dialog box.

Log details

Log details can be viewed for any of the collected logs. The details provided in vary depending on the device and type of log selected. The fields available in the this pane cannot be edited or re-organized.

To view log details, select the log in the log message list. Click the log details icon to the left of the limit field, the log details frame will be displayed in the lower frame of the content pane. Log details are not available when viewing raw logs.

In the *Log View* pane, select the *Tools* button, and select *Display Log Details* to enable log details display.

Archive

The *Archive* tab is displayed next to the *Log Details* tab in the lower content pane when archived logs are available. The archive icon is displayed in the log entry line to identify that an archive file is available.

The name and size of the archived log files are listed in the table. Selecting the download button next to the file name allows you to save the file to your computer.

Depending on the file type of the archived log file, the *View Packet Log* button may also be available next to the download button. Select this button to open the *View Packet Log* dialog box, which displays the path and content of the log file.

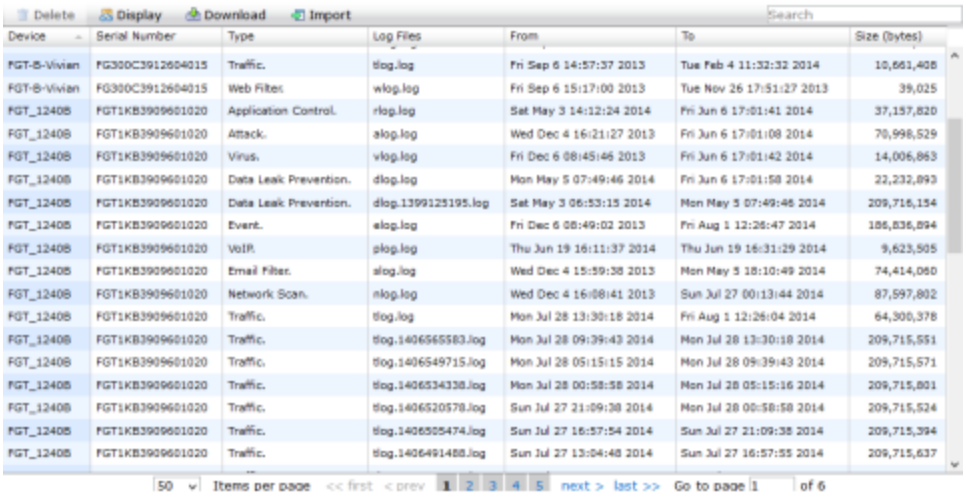
Browsing log files

Go to *FortiView* > *Log View* > *Log Browse* to view log files stored for devices. In this page you can display, download, delete, and import log files.

When a log file reaches its maximum size or a scheduled time, the FortiAnalyzer rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log`, where `x` is a letter indicating the log type, and `N` is a unique number corresponding to the time the first log entry was received.

For information about setting the maximum file size and log rolling options, see Configuring rolling and uploading of logs on page 142.

If you display the log messages in formatted view, you can perform all the same actions as with the log message list. See Viewing log messages on page 130.



This page displays the following:

Delete	Select the file of files whose log messages you want to delete, then select *Delete*, and then select *OK* in the confirmation dialog box.
Display	Select the file whose log messages you want to view, then select *Display* to open the log message list. For more information, see Viewing log messages on page 130

Download	Download a log file. See Downloading a log file on page 141.
Import	Import log files.
Search	Search the log files by entering a text value in the search window, such as a device serial number.
Log file list	A list of the log files.
Device	The device host name.
Serial Number	The device serial number.
Type	The log type. For example: *Email Filter*, *Event*, *Traffic*, *Web Filter*, *Virus*, *Application Control*, *Data Leak Prevention*, etc.
Log Files	A list of available log files for each device. The current, or active, log file appears as well as rolled log files. Rolled log files include a number in the file name, such as `vlog.1267852112.log`. If you configure the FortiAnalyzer unit to delete the original log files after uploading rolled logs to an FTP server, only the current log will exist.
From	The time when the log file began to be generated.
To	The time when the log file generation ended.
Size (bytes)	The size of the log file, in bytes.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.

Importing a log file

Imported log files can be useful when restoring data or loading log data for temporary use. For example, if you have older log files from a device, you can import these logs to the FortiAnalyzer unit so that you can generate reports containing older data.

Importing log files is also useful when changing your RAID configuration. Changing your RAID configuration will reformat the hard disk, erasing the log files. If you back up the log files, after changing the RAID configuration, you can import the logs to restore them to the FortiAnalyzer unit.

To import a log file:

1. Go to *FortiView* > *Log View* > *Log Browse*.
2. Select *Import* in the toolbar. The *Import Log File* dialog box opens.
3. Select the device to which the imported log file belongs from the *Device* field drop-down list, or select *[Take From Imported File]* to read the device ID from the log file. If you select *[Take From Imported File]* your log file must contain a `device_id` field in its log messages.
4. In the *File* field, select *Browse*. and find to the log file on the management computer.
5. Select *OK*. A message appears, stating that the upload is beginning, but will be cancelled if you leave the page.

6. Select *OK*. The upload time varies depending on the size of the file and the speed of the connection.
   After the log file has been successfully uploaded, the FortiAnalyzer unit will inspect the file:
   - If the `device_id` field in the uploaded log file does not match the device, the import will fail. Select *Return* to attempt another import.
   - If you selected *[Take From Imported File]*, and the FortiAnalyzer unit's device list does not currently contain that device, a message appears after the upload. Select *OK* to import the log file and automatically add the device to the device list.

Downloading a log file

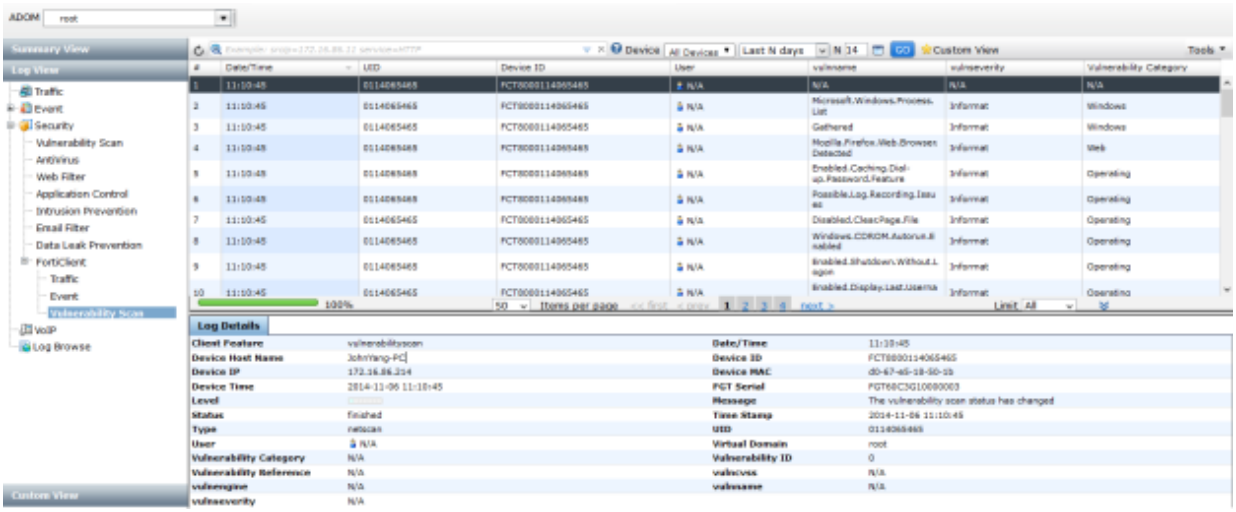
You can download a log file to save it as a backup or for use outside the FortiAnalyzer unit. The download consists of either the entire log file, or a partial log file, as selected by your current log view filter settings and, if downloading a raw file, the time span specified.

To download a log file:

1. Go to *FortiView* > *Log View* > *Log Browse*.
2. Select the specific log file that you need to download, then select *Download* from the toolbar. The *Download Log File* dialog box opens.
3. Select the log file format, either text, Native, or CSV.
4. Select *Compress with gzip* to compress the log file.
5. Select *Apply* to download the log file.
   If prompted by your web browser, select a location to where save the file, or open the file without saving.

FortiClient logs

The FortiAnalyzer unit can receive FortiClient logs uploaded through TCP port 514. FortiClient logs can be viewed downloaded from *Log View* > *FortiClient*.



To download a FortiClient log file, select the desired log from the list, then select *Download* from the Tools menu. In the confirmation dialog box, select if you want to compress the log file with gzip, then select *Apply* to download the log file.

For more information, see the *FortiClient Administration Guide*.

Configuring rolling and uploading of logs

You can control device log file size and use of the FortiAnalyzer unit's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiAnalyzer unit receives new log items, it performs the following tasks:

- verifies whether the log file has exceeded its file size limit
- checks to see if it is time to roll the log file if the file size is not exceeded.

Configure the time to be either a daily or weekly occurrence, and when the roll occurs. When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiAnalyzer unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog.1252929496.log`), where `x` is a letter indicating the log type and `N` is a unique number corresponding to the time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called `tlog.log`. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the GUI, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2012-09-29-08-03-54.gz
```

If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Log rolling and uploading can be enabled and configured in the GUI in *System Settings > Advanced > Device Log Settings*. For more information, see Device log settings on page 111. Log rolling and uploading can also be enabled and configured using the CLI. For more information, see the FortiAnalyzer CLI Reference.

To enable or disable log file uploads:

To enable log uploads, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload enable
      end
   end
```

To disable log uploads, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload disable
      end
   end
```

To roll logs when they reach a specific size:

Enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set file-size <integer>
      end
   end
```

where `<integer>` is the size at which the logs will roll, in MB.

To roll logs on a schedule:

To disable log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set when none
      end
   end
```

To enable daily log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload enble
      set when daily
      set hour <integer>
      set min <integer>
      set file-size <integer>
      end
   end
```

where:

`hour <integer>`	The hour of the day when the when the FortiAnalyzer rolls the traffic analyzer logs.
`min <integer>`	The minute when the FortiAnalyzer rolls the traffic analyzer logs.
`file-size <integer>`	Roll log files when they reach this size (MB).

To enable weekly log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set when weekly
      set days {mon | tue | wed | thu | fri | sat | sun}
      set hour <integer>
      set min <integer>
      end
   end
```

where:

`days {mon | tue | wed | thu | fri | sat | sun}`	The days week when the FortiAnalyzer rolls the traffic analyzer logs.
`hour <integer>`	The hour of the day when the when the FortiAnalyzer rolls the traffic analyzer logs.
`min <integer>`	The minute when the FortiAnalyzer rolls the traffic analyzer logs.

Event Management

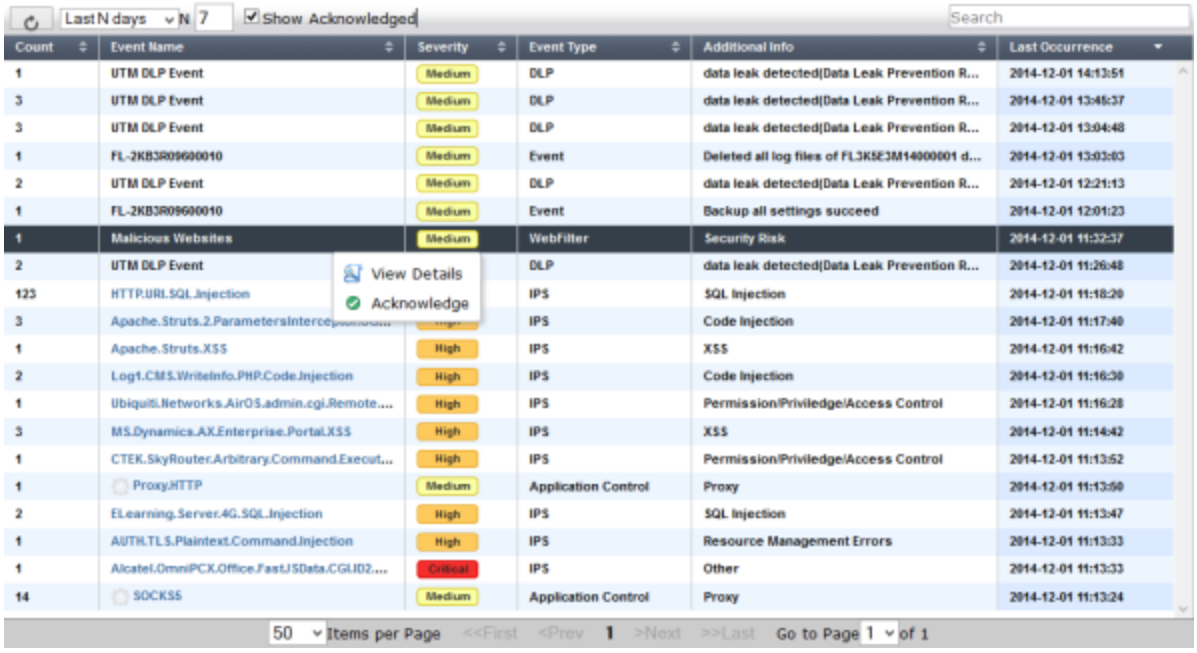
In the *Event Management* tab you can configure events handlers based on log type and logging filters. You can select to send the event to an email address, SNMP community, or syslog server. Events can be configured per device, for all devices, or for the local FortiAnalyzer. You can create event handlers for FortiGate and FortiCarrier devices. In 5.0.7 or later, Event Management supports local FortiAnalyzer event logs.

Events can also be monitored, and the logs associated with a given event can be viewed.

Events

The events page provides a list of the generated events. Right-clicking on an event in the table gives you the option of viewing event details including the raw log entries associated with that event, adding review notes, and acknowledging the event.

To view events, go to the *Event Management* tab and select *Event Management* > *All Events*. You can also view events by severity and by handler. When ADOMs are enabled, select the ADOM, and then select *All Events*.



The following information is displayed:

Refresh	Select to refresh the entries displayed.

Time Period	Select a time period from the drop-down list. Select one of: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, *All*. If applicable, enter the number of days or hours for N in the *N* text box.
Show Acknowledged	Select to show or hide acknowledged events. Acknowledged events are greyed out in the list.
Search	Search for a specific event.
Count	The number of log entries associated with the event. Click the heading to sort events by count.
Event Name	The name of the event. Click the heading to sort events by event name.
Severity	The severity level of the event. Event severity level is a user configured variable. The severity can be *Critical*, *High*, *Medium*, or *Low*. Click the heading to sort events by severity.
Event Type	The event type. For example, *Traffic* or *Event*. Click the heading to sort events by event type.
Additional Info	Additional information about the event. Click the heading to sort events by additional information.
Last Occurrence	The date and time that the event was created and added to the events page. Click the heading to sort events by last occurrence.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.

Right-click on an event in the list to open the right-click menu. The following options are available:

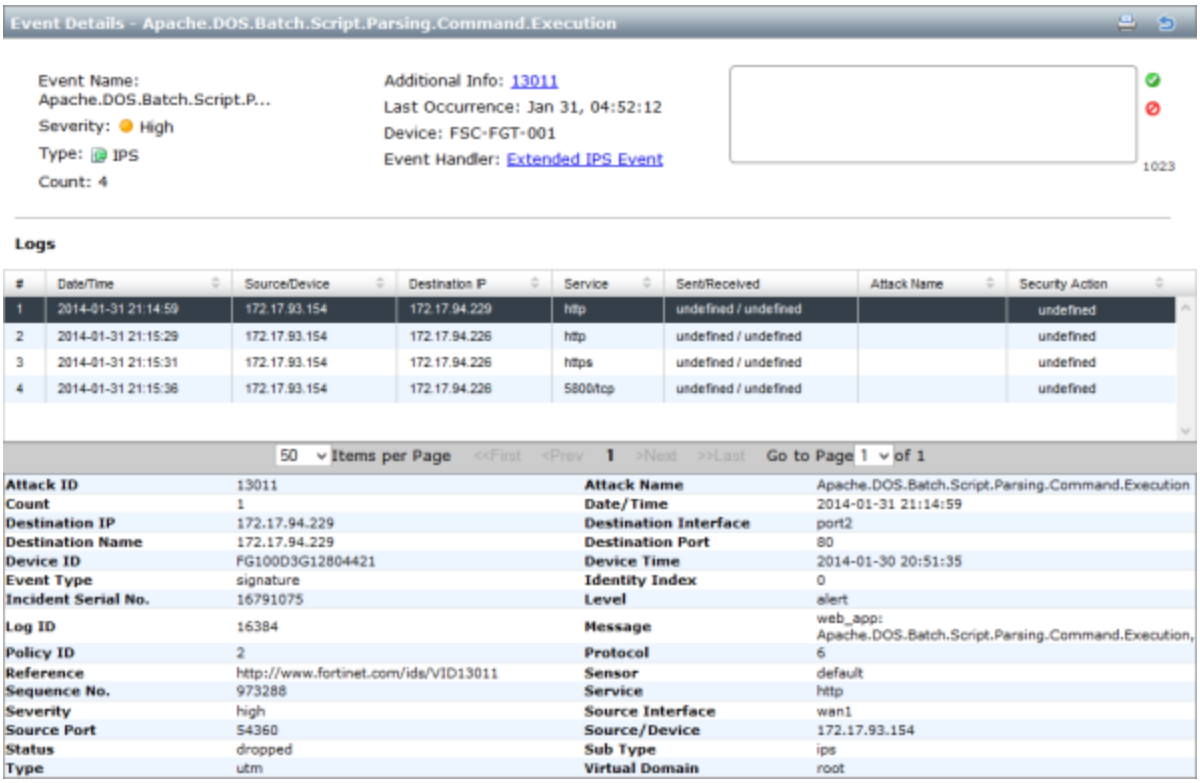
View Details	The *Event Details* page is displayed. This option is available in the right-click menu.
Acknowledge	Acknowledge an event. If *Show Acknowledge* is not selected, the event will be hidden. See Acknowledge events on page 147.

Event details

Event details provides a summary of the event including the event name, severity, type, count, additional information, last occurrence, device, event handler, raw log entries, and review notes. You can also acknowledge and print events in this page.

To view log messages associated with an event:

1. In the events list, either double-click on an event or right-click on an event then select *View Details* in the right-click menu. The *Event Details* page opens.



2. The following information and options are available:

Print	Select the print icon to print the event details page. The log details pane is not printed.
Return	Select the return icon to return to the *All Events* page.
Event Name	The name of the event, also displayed in the title bar.
Severity	The severity level configured for the event handler.
Type	The event category of the event handler.
Count	The number of logged events associated with the event.
Additional Info	This field either displays additional information for the event or a link to the FortiGuard Encyclopedia. A link will be displayed for Antivirus, Application Control, and IPS event types.
Last Occurrence	The date and time of the last occurrence.
Device	The device hostname associated with the event.
Event Handler	The name of the event handler associated with the event. Select the link to edit the event handler. See Event handler on page 147.

Text box	Optionally, you can enter a 1023 character comment in the text field. Select the save icon to save the comment, or cancel to cancel your changes.
Logs	The logs associated with the log event are displayed. The columns and log fields are dependent on the event type.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.
Log details	Log details are shown in the lower content pane for the selected log. The details will vary based on the log type.

3. Select the return icon to return to the *All Events* page.

Acknowledge events

You can select to acknowledge events to remove them from the event list. An option has been added to this page to allow you to show or hide these acknowledged events.

To acknowledge events:

1. From the event list, select the event or events that you would like to acknowledge.
2. Right-click and select *Acknowledge* in the right-click menu.
3. Select the *Show Acknowledge* checkbox in the toolbar to view acknowledged events.

Event handler

The event handler allows you to view, create new, edit, delete, clone, and search event handlers. You can select these options in the toolbar. The right-click menu includes these options and also includes the ability to enable or disable configured event handlers. You can create event handlers for a specific device, multiple devices, or the local FortiAnalyzer. You can select to create event handlers for traffic logs or event logs.

FortiAnalyzer 5.0.7 or later includes default event handlers for FortiGate and FortiCarrier devices. Click on the event handler name to enable or disable the event handler and to assign devices to the event handler.

Event Handler	Description
Antivirus Event	**Definition** • Severity: High • Log Type: Traffic Log • Event Category: AntiVirus • Group by: Virus Name • Log messages that match all conditions: • *Level Greater Than or Equal To Information* **Notification** Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

App Ctrl Event	**Definition**
	• Severity: Medium
	• Log Type: Traffic Log
	• Event Category: Application Control
	• Group by: Application Name
	• Log messages that match any of the following conditions:
	  • *Application Category Equal To Botnet*
	  • *Application Category Equal To Proxy*
	Notification
	Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes.
	Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

DLP Event	**Definition** • Severity: Medium • Log Type: Traffic Log • Event Category: DLP • Group by: DLP Rule Name • Log messages that match all conditions: • *Security Action Equal To Blocked* **Notification** Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

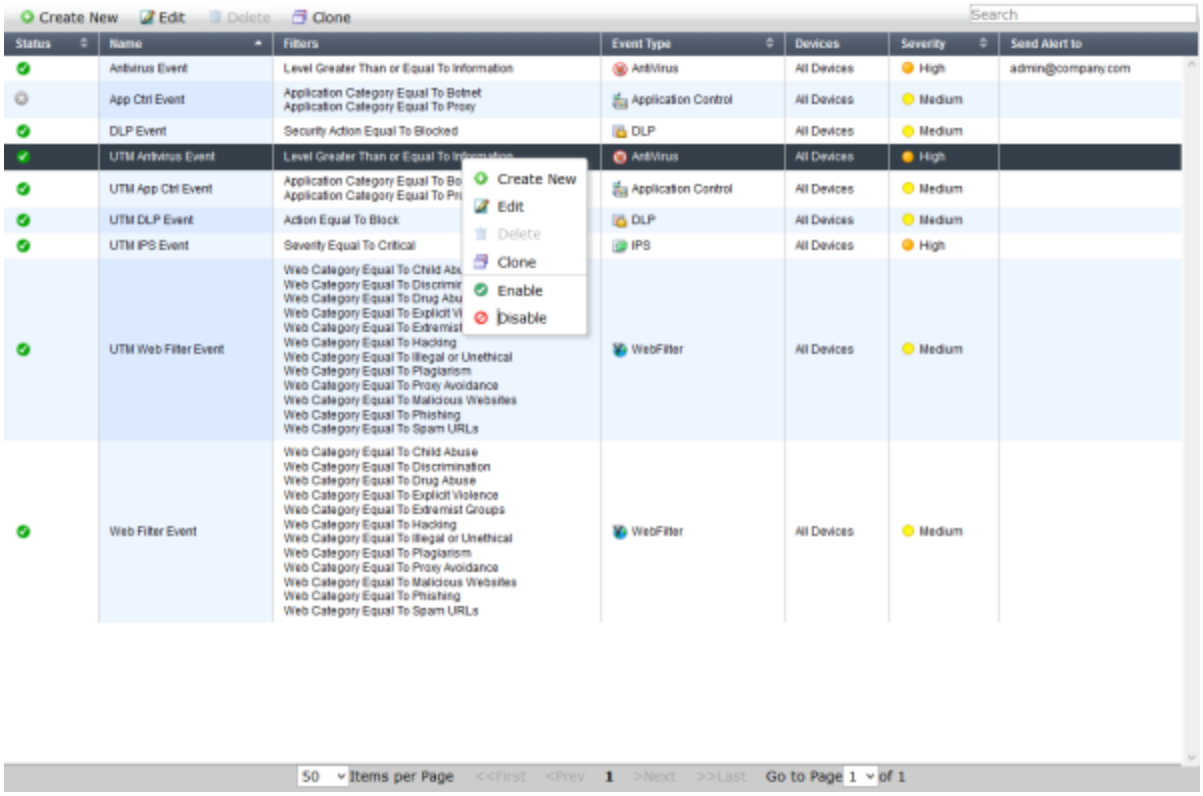
Event Handler	Description
UTM Antivirus Event	**Definition** • Severity: High • Log Type: Virus • Group by: Virus Name • Log messages that match all conditions: • *Level Greater Than or Equal To Information* **Notification** Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

UTM App Ctrl Event	**Definition**
	• Severity: Medium
	• Log Type: Application Control
	• Group by: Application Name
	• Log messages that match any of the following conditions:
	  • *Application Category Equal To Botnet*
	  • *Application Category Equal To Proxy*
	Notification
	Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes.
	Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

UTM DLP Event	**Definition** • Severity: Medium • Log Type: DLP • Group by: DLP Rule Name • Log messages that match all conditions: • *Action Equal To Block* **Notification** Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

Event Handler	Description
UTM IPS Event	**Definition** • Severity: High • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To Critical* **Notification** Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.
UTM Web Filter Event	**Definition** • Severity: Medium • Log Type: Web Filter • Group by: Category • Log messages that match any of the following conditions: • *Web Category Equal To Child Abuse*, *Discrimination*, *Drug Abuse*, *Explicit Violence*, *Extremist Groups*, *Hacking*, *Illegal or Unethical*, *Plagiarism*, *Proxy Avoidance*, *Malicious Websites*, *Phishing*, *Spam URLs* **Notification** Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.
Web Filter Event	**Definition** • Severity: Medium • Log Type: Traffic Log • Event Category: WebFilter • Group by: Category • Log messages that match any of the following conditions: • *Web Category Equal To Child Abuse*, *Discrimination*, *Drug Abuse*, *Explicit Violence*, *Extremist Groups*, *Hacking*, *Illegal or Unethical*, *Plagiarism*, *Proxy Avoidance*, *Malicious Websites*, *Phishing*, *Spam URLs* **Notification** Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

Go to the *Event Management* tab and select *Event Handler* in the tree menu.



The following information is displayed:

Status	The status of the event handler (enabled or disabled).
Name	The name of the event handler.
Filters	The filters that are configured for the event handler.
Event Type	The event category of the event handler. The information displayed is dependent on the platform type.
Devices	The devices that you have configured for the event handler. This field will either display *All Devices* or list each device. When you have configured an event handler for local logs, *Local FortiAnalyzer* will be displayed.
Severity	The severity that you configured for the event handler. This field will display *Critical, High, Medium*, or *Low*.
Send Alert to	The email address, SNMP server, or syslog server that has been configured for the event handler.

Right-click on an event handler in the list to open the right-click menu. The following options are available:

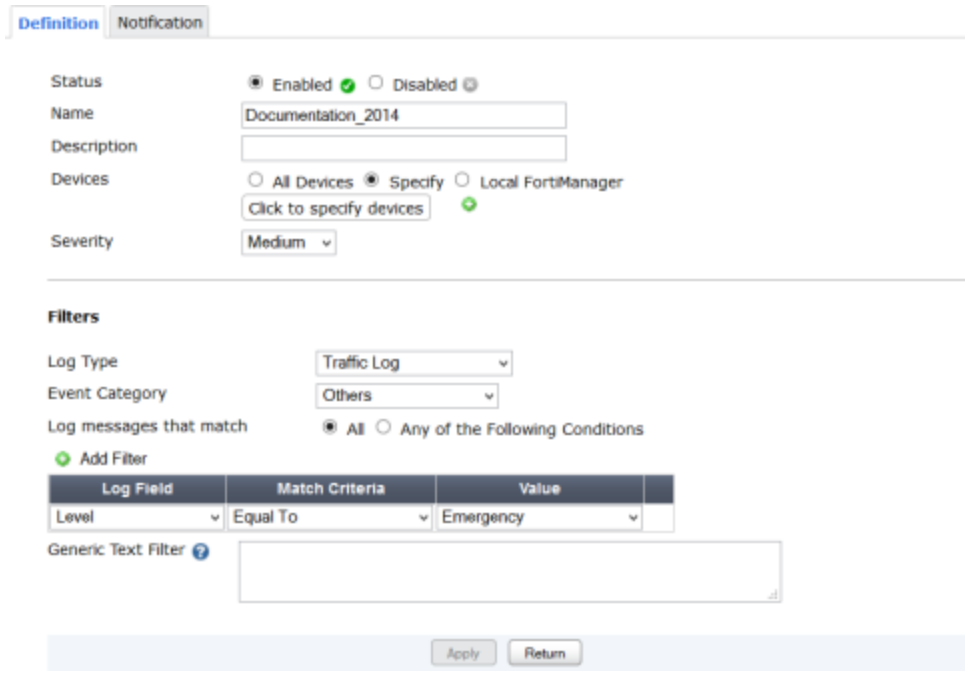
Create New	Select to create a new event handler. This option is available in the toolbar and right-click menu.
Edit	Select an event handler and select edit to make changes to the entry. This option is available in the toolbar and right-click menu.
Delete	Select one or all event handlers and select delete to remove the entry or entries. This option is available in the toolbar and right-click menu. The default event handlers cannot be deleted.
Clone	Select an event handler in this page and click to clone the entry. A cloned entry will have *Copy* added to its name field. You can rename the cloned entry while editing the event handler. This option is available in the toolbar and right-click menu.
Enable	Select to enable the event handler.
Disable	Select to disable the event handler.

Manage event handlers

You can create traffic, event, and extended log handlers to monitor network traffic and events based on specific log filters. These log handlers can then be edited, deleted, cloned, and enabled or disabled as needed.

To create a new event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select *Create New* in the toolbar, or right-click on an the entry and select *Create New* in the right-click menu. The *Create New Event Handler* dialog box is displayed.
3. Enter a name for the new event handler and select *OK*. The *Event Handler* page opens with the *Definition* tab displayed.

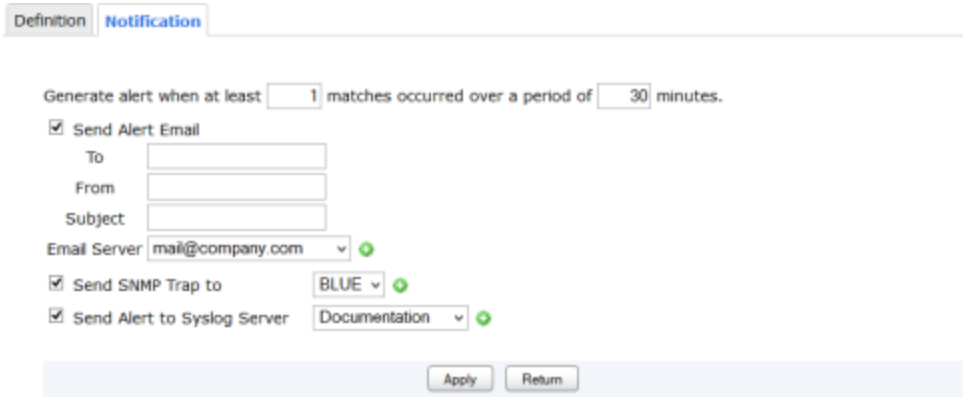


4. Configure the following settings:

Status	Enable or disable the event handler.
Name	Edit the name if required.
Description	Enter a description for the event handler.
Devices	Select *All Devices*,select *Specify* and use the add icon to add devices. Select *LocalFortiAnalyzer* if the event handler is for local FortiAnalyzer event logs. Local FortiAnalyzer is available in the root ADOM only and is used to query FortiAnalyzer event logs.
Severity	Select the severity from the drop-down list. Select one of the following: *Critical*, *High*, *Medium*, or *Low*.
Filters	
Log Type	Select the log type from the drop-down list. The available options are: *Traffic Log*, *Event Log*, *Application Control*, *DLP*, *IPS*, *Virus*, and *Web Filter*. The *Log Type* is *Event Log* when *Devices* is *Local FortiAnalyzer*.
Event Category	Select the category of event that this handler will monitor from the drop-down list: *AntiVirus*, *Application Control*, *DLP*, *IPS*, *Web Filter*, or *Others*.This option is only available when *Log Type* is set to *Traffic Log* and *Devices* is set to either *All Devices* or *Specify*.
Group by	Select the criterium by which the information will be grouped. This option is not available when *Log Type* is set to *Traffic Log*.

Log message that match	Select either *All* or *Any of the Following Conditions*. When *Devices* is *Local FortiAnalyzer* this option is not available.
Add Filter	Select the add icon to add log filters. When *Devices* is *Local FortiAnalyzer*, this option is not available. You can only set one log field filter.
Log Field	Select a log field to filter from the drop-down list. The available options will vary depending on the selected log type.
Match Criteria	Select a match criteria from the drop-down list. The available options will vary depending on the selected log field.
Value	Either select a value from the drop-down list, or enter a value in the text box. The available options will vary depending on the selected log field.
Delete	Select the delete icon, to delete the filter. A minimum of one filter is required.
Generic Text Filter	Enter a generic text filter. For more information on creating a text filter, hover the cursor over the help icon.

5. Select *Apply* to save the *Definition* settings.
6. Select the *Notification* tab.



7. Configure the following settings:

Generate alert when at least	Enter threshold values to generate alerts. Enter the number, in the first text box, of each type of event that can occur in the number of minutes entered in the second text box.
Send Alert Email	Select the checkbox to enable. Enter an email address in the *To* and *From* text fields, enter a subject in the *Subject* field, and select the email server from the drop-down list. Select the add icon to add an email server. For information on creating a new mail server, see Mail server on page 109.
Send SNMP Trap to	Select the checkbox to enable this feature. Select an SNMP community from the drop-down list. Select the add icon to add a SNMP community

Send Alert to Syslog Server	Select the checkbox to enable this feature. Select a syslog server from the drop-down list. Select the add icon to add a syslog server. For information on creating a new syslog server, see Syslog server on page 109

8. Select *Apply* to create the new event handler.
9. Select *Return* to return to the *Event Handler* page.

To edit an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Edit* in the toolbar, or right-click on the entry and select *Edit* in the pop-up menu. The *Edit Event Handler* page opens.
3. Edit the settings as required.
4. Select *Apply* to save the configuration.
5. Select *Return* to return to the *Event Handler* page.

To clone an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Clone* in the toolbar, or right-click on the entry and select *Clone* in the pop-up menu. The *Clone Event Handler* window opens.
3. Edit the settings as required.
4. Select *Apply* to save the configuration.
5. Select *Return* to return to the *Event Handler* page.

To delete an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Delete* in the toolbar, or right-click on the entry and select *Delete* in the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the event handler.

The default event handlers cannot be deleted. Use the right-click menu to enable or disable these event handlers. You can also select to clone the default event handlers.

To enable an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry, right-click and select *Enable* in the pop-up menu. The status field will display a enabled icon.

To disable an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry, right-click and select *Disable* in the pop-up menu. The status field will display a disabled icon.

Reports

FortiAnalyzer units can analyze information collected from the log files of managed log devices. It then presents the information in tabular and graphical reports that provide a quick and detailed analysis of activity on your networks.

To reduce the number of reports needed, reports are independent from devices, and contain layout information in the form of a report template. The devices, and any other required information, can be added as parameters to the report at the time of report generation.

Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the GUI page to access these options.

The *Reports* tab allows you to configure reports using the predefined report templates, configure report schedules, view report history and the report calendar, and configure and view charts, macros, datasets, and output profiles.

If ADOMs are enabled, each ADOM will have its own report settings including chart library, macro library, dataset library, and output profiles.
FortiMail and FortiWeb reports are available when ADOMs are enabled. Reports for these devices are configured within their respective default ADOM. FortiMail and FortiWeb have device specific charts and datasets.

The Reports tab is available when the FortiAnalyzer operation mode is Analyzer.

When rebuilding the SQL database, Reports will not be available until after the rebuild is completed. The progress of the rebuild will be shown in the title bar.

This chapter contains the following sections:

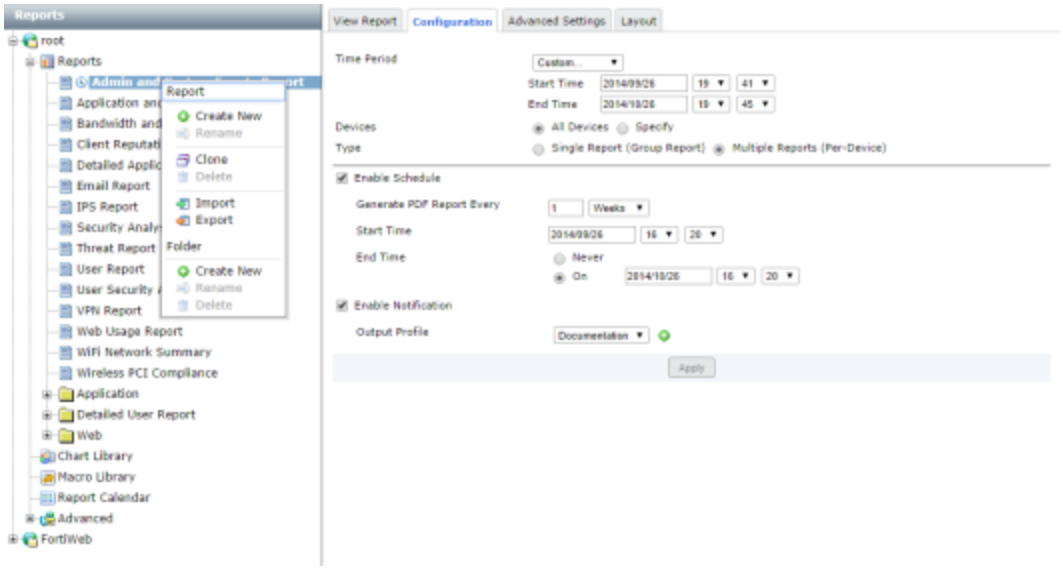
- Reports
- Report layouts
- Chart library
- Macro library
- Report calendar
- Advanced

Reports

FortiAnalyzer includes preconfigured reports and report templates for FortiGate, FortiMail, and FortiWeb log devices. These report templates can be used as is, or you can clone and edit the templates. You can also create new reports and report templates that can be customized to your requirements.

Predefined report templates are identified by a blue report icon and custom report templates are identified by a green report icon. When a schedule has been enabled, the schedule icon will appear to the left of the report template name.

In the *Reports* tab, go to *Reports* > *[report]* to view and configure the report configuration, advanced settings, and layout, and to view completed reports. The currently running reports and completed reports are shown in the *View Report* tab, see View report tab on page 163.



Right-clicking on a template in the tree menu opens a pop-up menu with the following options:

Report		
	Create New	Create a new report. Custom report templates are identified by the custom report icon beside the report name. Predefined report templates are identified by the predefined report icon, .
	Rename	Rename a report.
	Clone	Clone the selected report.
	Delete	Delete the report. The default reports cannot be deleted.
	Import	Import a report.
	Export	Export a report.
Folder		
	Create New	Create a new report folder.
	Rename	Rename a report folder.
	Delete	Delete a report folder. Any report templates in the folder will be deleted.

Reports and report templates can be created, edited, cloned, and deleted. You can also import and export report templates. New content can be added to and organized on a template, including: new sections, three levels of headings, text boxes, images, charts, and line and page breaks.

To create a new report:

1. In the *Reports* tab, right-click on *Reports* in the tree menu.
2. Under the *Report* heading, select *Create New*. The *Create New Report* dialog box opens.
3. Enter a name for the new report and select *OK*.
4. Configure report settings in the Configuration tab. The configuration tab includes time period, device selection, report type, schedule, and notifications.

To create a custom cover page, you must select *Print Cover Page* in the *Advanced Settings* menu in the *Advanced Settings* tab.

5. Select the Report layouts to configure the report template.
6. Select the Advanced settings tab to configure report filters and other advanced settings.
7. Select *Apply* to save the report template.

To clone a report:

1. Right-click on the report you would like to clone in the tree menu and select *Clone*. The *Clone Report Template* dialog box opens.
2. Enter a name for the new template, then select *OK*.

   A new template with the same information as the original template is created with the given name. You can then modify the cloned report as required.

To delete a report:

1. Right-click on the report template that you would like to delete in the tree menu, and select *Delete* under the *Report* heading.
2. In the confirmation dialog box, select *OK* to delete the report template.

Import and export

Report templates can be imported from and exported to the management computer.

To import a report template:

1. Right-click on *Reports*, and select *Import*. The *Import Report Template* dialog box opens.
2. Select *Browse*, locate the report template (.dat) file on your management computer, and select *OK*.

   The report template will be loaded into the FortiAnalyzer unit.

To export a report template:

1. Right-click on the report you would like to export in the tree menu and select *Export*.
2. If a dialog box opens, select to save the file (.dat) to your management computer, and select *OK*.

   The report template can now be imported to another FortiAnalyzer device.

Report folders

Report folders can be used to help organize your reports.

To create a new report folder:

1. In the *Reports* tab, right-click on *Reports* in the tree menu.
2. Under the *Folder* heading, select *Create New*.
3. In the *Create New Folder* dialog box, enter a name for the folder, and select *OK*.
   A new folder is created with the given name.

To rename a report folder:

1. Right-click on the report folder that you need to rename in the tree menu.
2. Under the *Folder* heading, select *Rename*.
3. In the *Rename Folder* dialog box, enter a new name for the folder, and select *OK*.

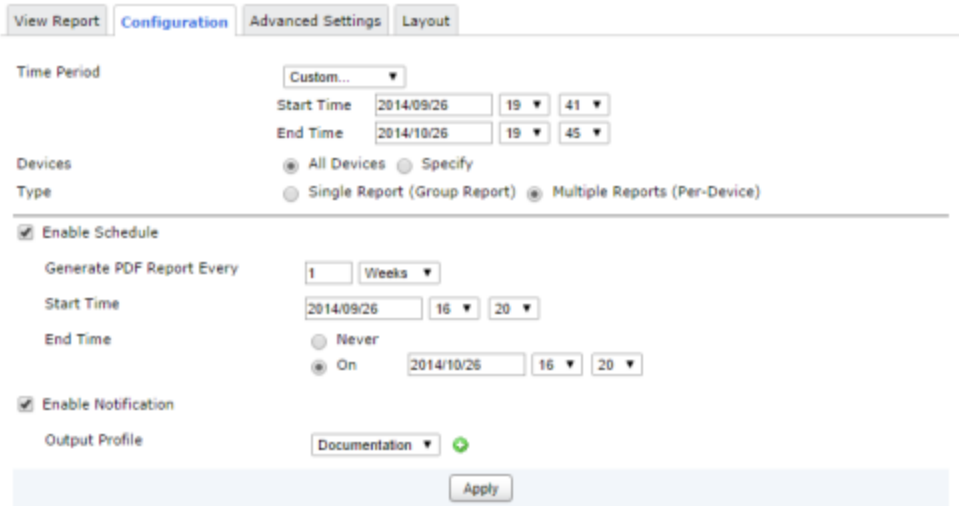
To delete a report folder:

1. Right-click on the report folder that you would like to delete in the tree menu, and select *Delete* under the *Folder* heading.
2. In the confirmation dialog box, select *OK* to delete the report folder.

Configuration tab

In FortiAnalyzer v5.0.7 or later, the Reports module layout has changed. When creating a new report, the *Configuration* tab is the first tab that is displayed. In this tab you can configure the time period, select devices, enable schedules, and enable notification.

Report schedules provide a way to schedule an hourly, daily, weekly, or monthly report so that the report will be generated at a specific time. You can also manually run a report schedule at any time, and enable or disable report schedules. Report schedules can also be edited and disabled from the *Report Calendar*. See Report calendar on page 184 for more information.

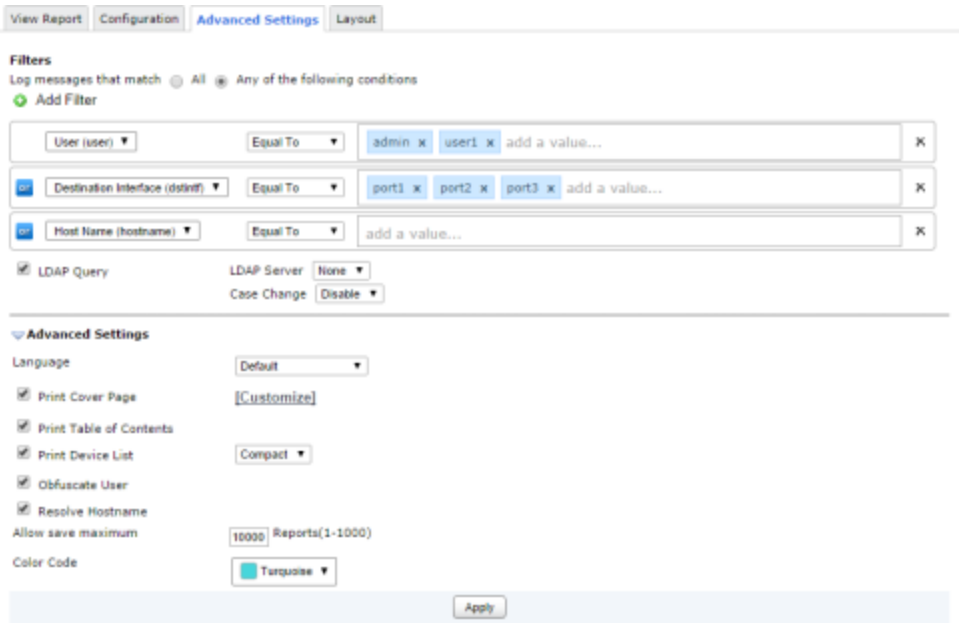


The following settings are available in the *Configuration* tab:

Time Period	The time period that the report will cover. Select a time period, or select *Custom* to manually specify the start and end date and time.
Devices	The devices that the report will include. Select either *All Devices or Specify* to add specific devices. Select the add icon to select devices.
User or IP	Select to add a user filter. Select the add icon and then enter the user name or IP address in the text field. You can add multiple user filters. This field is only available for the three predefined report templates in the *Detailed User Report* folder.
Type	Select either *Single Report (Group Report)* or *Multiple Reports (Per-Device)*. This option is only available if multiple devices are selected.
Enable Schedule	Select to enable report template schedules.
Generate PDF Report Every	Select when the report is generated. Enter a number for the frequency of the report based on the time period selected from the drop-down list.
Starts On	Enter a starting date and time for the file generation.
Ends	Enter an ending date and time for the file generation, or set it for never ending.
Enable Notification	Select to enable report notification.
Output Profile	Select the output profile from the drop-down list, or select the create new icon to create a new output profile. See Output profile on page 189.

Advanced settings tab

After configuring the report configuration, select the *Advanced Settings* tab. In this tab you can configure report filters, LDAP query, and other advanced settings. In the filters section of the *Configuration* tab, you can create and apply log message filters, and add an LDAP query to the report. The *Advanced Settings* section allows you to configure language and print options, and other settings.In this section of the report, you can configure report language, print and customize the cover page, print the table of contents, print a device list, and obfuscate users.



The following settings are available in the *Advanced Settings* tab:

Filters		In the filters section of the *Configuration* tab, you can create and apply log message filters, and add an LDAP query to the report. Use the search field to find a specific filter.
	Log messages that match	Select *All* to filter log messages based on all of the added conditions, or select *Any of the following conditions* to filter log messages based on any one of the conditions.
	Add Filter	Select to add filters. For each filter, select the field, and operator from the drop-down lists, then enter or select the value as applicable. In v5.0.8 and later, you can enter multiple values. Filters vary based on device type.
	LDAP Query	Select the checkbox to add an LDAP query, then select the LDAP server and the case change value from the drop-down lists.
Advanced Settings		Configure advanced report settings.
	Language	Select the report language. Select one of the following: *English*, *French*, *Japanese*, *Korean*, *Portuguese*, *Simplified_Chinese*, *Spanish*, or *Traditional_Chinese*.
	Print Cover Page	Select the checkbox to print the report cover page. Select *Customize* to customize the cover page.
	Print Table of Contents	Select the checkbox to include a table of contents.

	Print Device List	Select the checkbox to print the device list. Select *Compact*, *Count*, or *Detailed* from the drop-down list.
	Obfuscate User	Select the checkbox to hide user information in the report.
	Resolve Host-name	Select the checkbox to resolve hostnames in the report. The default status is enabled.
	Allow save max-imum	Select a value between 1-1000 for the maximum number of reports to save.
	Color Code	The color used to identify the report on the calendar. Select a color code from the drop-down list to apply to the report schedule. Color options include: *Bold Blue*, *Blue*, *Turquoise*, *Green*, *Bold Green*, *Yellow*, *Orange*, *Red*, *Bold Red*, *Purple*, and *Gray*.

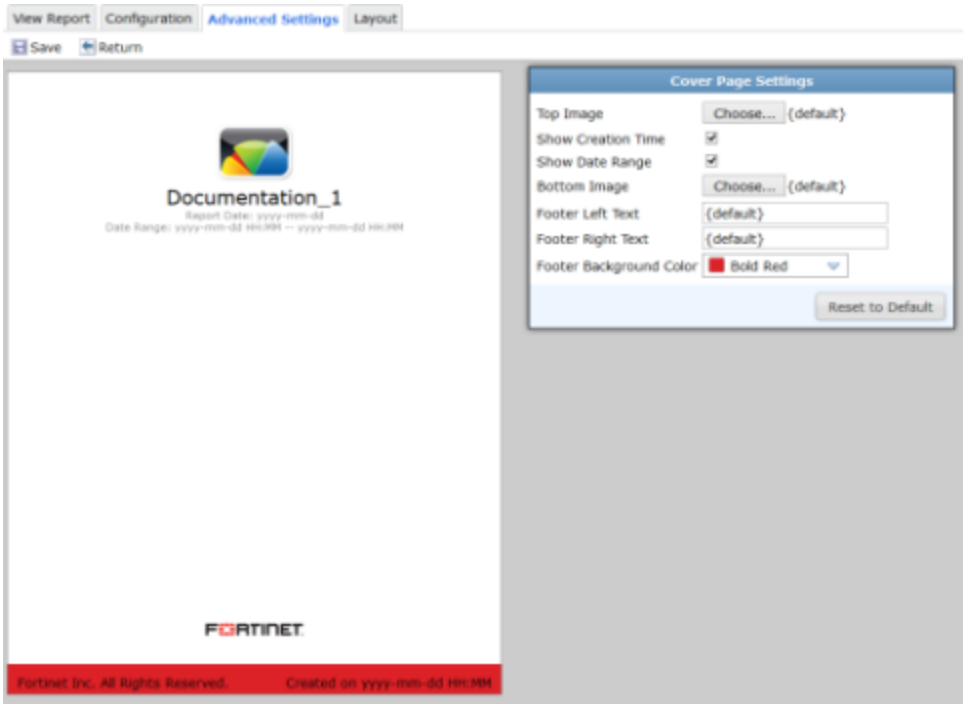
Report cover pages

The report cover page is only included in the report when enabled in the *Advanced Settings* menu in the *Advanced Settings* tab. See Advanced settings tab on page 160.

When enabled, the cover page can be edited to contain the desired information and imagery.

To edit cover page settings:

1. In the *Reports* tab, select the report in the tree menu whose cover page you are editing, then select the *Advanced Settings* tab.
2. In the *Advanced Settings* section, select *Customize* next to the *Print Cover Page* option. The *Cover Page Settings* page opens.



3. Configure the following settings:

Top Image	Select *Choose* to open the *Choose a graphic* dialog box. Select an image, or select *Upload* to find an image on the management computer, then select *OK* to add the image at the top of the cover page.
Show Creation Time	Select the checkbox to print the report date on the cover page.
Show Data Range	Select the checkbox to print the data range on the cover page.
Bottom Image	Select *Choose* to open the *Choose a graphic* dialog box. Select an image, or select *Upload* to find an image on the management computer, then select *OK* to add the image at the bottom of the cover page.
Footer Left Text	Edit the text printed in the left hand footer of the cover page.
Footer Right Text	Edit the text printed in the left hand footer of the cover page. `{default}` prints the report creation date and time.
Footer Background Color	Select the cover page footer background color from the drop-down list.
Reset to Default	Select to reset the cover page settings to their default settings.

4. Select *Save* in the toolbar, to save your changes.
5. Select *Return* in the toolbar, to return to *Advanced Settings* tab.

View report tab

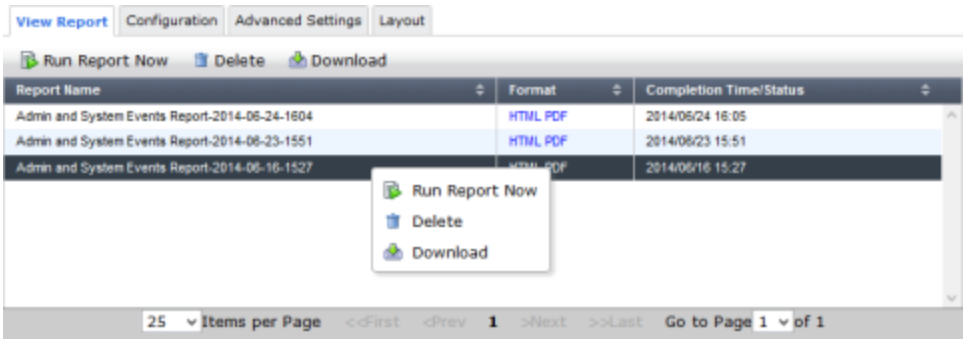
A report can be manually run at any time by selecting *Run Report Now*.

Competed reports are displayed in the *View Report* tab of the *Reports* tab. The report name, available formats, and completion time or status are shown in the table. Reports can be viewed in HTML or as PDFs.

The toolbar and the right-click menu provide options to delete or download the selected reports, as well as to run the report.

Completed reports can be viewed for specific devices from the *Device Manager* tab.

Completed reports can also be downloaded and deleted from the *Report Calendar* page. See Report calendar on page 184.



The following options are available:

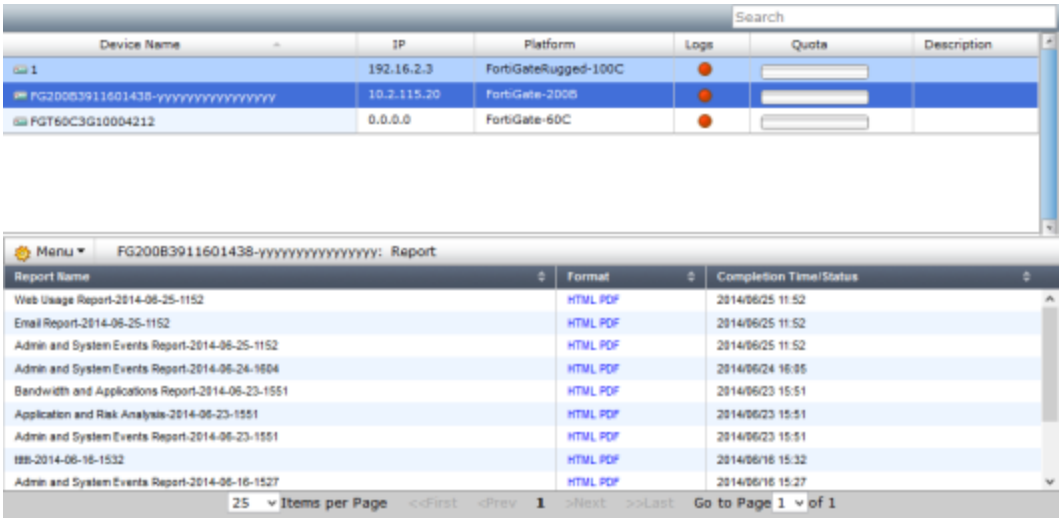
Report Name	The name of the report. Click the column header to sort entries in the table by report name.
Format	Select *HTML* to open the report in HTML format in a new web browser tab or window, depending on your browser settings. Select *PDF* to open or download the report in PDF format.
Completion Time/Status	The completion status of the report, or, if the report is complete, the data, and time (including time zone) that the report completed. Click the column header to sort entries in the table by completion time.

Right-click on an report in the list to open the right-click menu. The following options are available:

Run Report Now	Select to run the report now.
Delete	Select one or more reports in the completed reports list, then select *Delete* from the toolbar or right-click menu. Select *OK* in the confirmation dialog box to delete the selected report or reports.
Download	Select one reports in the completed reports list, then select *Download* from the toolbar or right-click menu to download the selected report or reports. Each report will be saved individually as a PDF file on the management computer. Reports that are not done cannot be downloaded.

To view device reports:

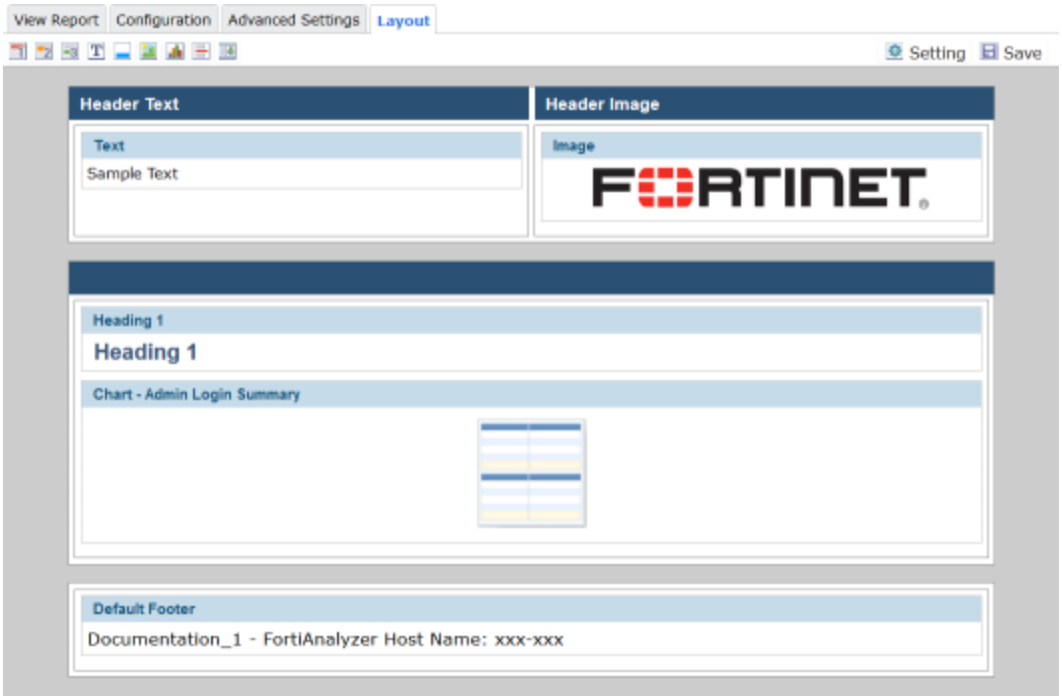
1. In the *Device Manager* tab, select the ADOM that contains the device whose report you would like to view. All of the reports that have been run for the selected device are shown in the lower content pane. See Device Manager on page 39.



2. Select a format from the *Format* column to open the report in that format in a new browser window or tab.
3. Select a report, then select *Download* from the right-click menu to download the selected report.
4. Select one or more reports, then select *Delete* to delete the selected reports.

Report layouts

In the *Layout* tab, you can configure report template settings and layout. Various content can be added to a report template, such as sections, charts, images, and typographic elements, using the layout toolbar. The template color scheme, fonts, and layout can be controlled, and all the report sections and elements can be edited and customized as needed.



The following options are available:

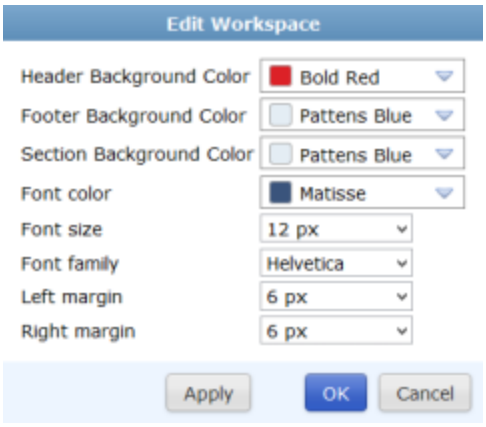
Elements	Add elements to the report template. See Elements on page 168.
Settings	Adjust the template workspace. See Workspace settings on page 165.
Save	Save your template changes.

Workspace settings

The report template workspace controls the colors, fonts, alignment, and margins of the report.

To edit the template workspace:

1. Select the workspaces *Setting* in the layout tab toolbar. The *Edit Workspace* dialog box opens.



2. Configure the following settings:

Header Background Color	Select the background color for the header from the drop-down list.
Footer Background Color	Select the background color for the footer from the drop-down list.
Section Background Color	Select the background color for sections from the drop-down list.
Font color	Select the font color from the drop-down list.
Font size	Enter the font size. The default size is 12 px.
Font family	Select one of the following: *Courier*, *Helvetica*, *Times*, *SimSun*, *SimHei*, *MingLiu*, *MS-Gothic*, *MS-PGothic*, *MS-Mincyo*, *MS-PMincyo*, *DotumChe*, *Dotum*, *BatangChe*, or *Batang*.
Left margin	Select the left margin value from the drop-down list.
Right margin	Select the right margin value from the drop-down list.

3. Select *Apply* or *OK* to apply your changes.

Sections

Report template sections contain report elements. By default, a blank report contains sections for header text, a header image, and a footer that cannot be removed. One blank section for content is included.

Elements can be added to, removed from, and organized in the blank section. Sections can be added, moved, edited, and removed using the section toolbar that appears when you hover the cursor over the section title bar, .

The following options are available in the section toolbar:

Add	Add a new section to the report template.
Move Up	Move the section above the section currently directly above it.

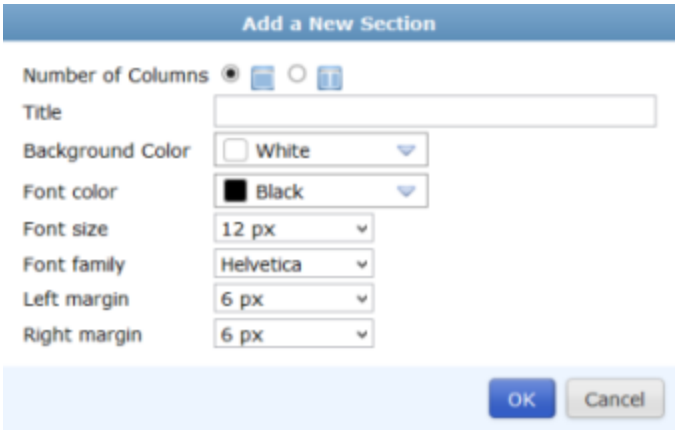
Move Down	Move the section below the section currently directly below it.
Edit	Edit the section.
Delete	Delete the section. Select *OK* in the confirmation dialog box. All section content will also be deleted.

Section specific settings will overwrite the workspace settings if configured after the workspace. To revert to the workspace settings, reconfigure the workspace. See Workspace settings on page 165.

The header text and header image will print the cover page information, including the device hostname, in the report header when selecting not to print the report cover page from the *Advanced Settings* tab.

To add a section to a report template:

1. From any content section toolbar, select the *Add a New Section* icon. The *Add a New Section* dialog box opens.



2. Configure the following settings:

Number of Columns	Select either one column, or two columns.
Title	Enter a title for the section (optional).
Background Color	Select the background color from the drop-down list.
Font color	Select the font color from the drop-down list.
Font size	Select the font size from the drop-down list. The default is 12 px.
Font family	Select one of the following: *Courier*, *Helvetica*, *Times*, *SimSun*, *SimHei*, *MingLiu*, *MS-Gothic*, *MS-PGothic*, *MS-Mincyo*, *MS-PMincyo*, *DotumChe*, *Dotum*, *BatangChe*, or *Batang*.
Left margin	Select the left margin value from the drop-down list.

Right margin	Select the right margin value from the drop-down list.

3. Select *OK* to create the new section.

To edit a section:

1. From any content section toolbar, select the *Edit Section* icon. The *Edit Section* dialog box opens.
2. Configure the section settings as required.
3. Select *OK* to edit the section.

Selecting *Apply* will reset customized color, font, and margin configurations in *Workspace* settings.

Elements

Elements can be added to sections in a report template by clicking and dragging the element's icon from the template toolbar to the location in the template where you want the element to appear.

The default sections will only accept certain elements:

- *Header Text* will only accept a single text element.
- *Header Image* will only accept a single image element.
- The footer section will only accept a single text element or the default footer element.

The following elements are available in the template toolbar:

Headings	Add one of three levels of headings to the template.
Text	Add a text box to the template.
Default Footer	The default footer can only be added to the footer or header text sections of the template. It includes the report name and the FortiAnalyzer host name.
Image	Add an image to the template.
Charts	Add a chart to the template.
Breaks	Add a line or page break to the template.

To move an element:

To move an element that has already been placed in the template, simply click and drag the element to the new location. A gray box with a dashed red outline will appear in the location where the element will be placed.

If you accidentally drag the element to a location where it does not fit, such as dragging an image into the footer section, the element will return to its previous location.

To delete an element:

To delete an element from the template, select delete icon in the element toolbar, then select *OK* in the confirmation dialog box.

Headings

Three heading levels are available and can be added to content sections within the report template. Heading settings, such as font and color, take precedence over section and workspace settings.

To add headings:

Click and drag the required heading icon from the template toolbar to the location in the content section where you want to add the heading.

To edit headings:

1. Select the edit icon in the heading toolbar to open the *Edit Heading* dialog box.
2. Configure the following settings:

Content	Enter the heading text.
Font color	Select the font color from the drop-down list.
Font size	Select the font size from the drop-down list.
Font family	Select the font family to use for the heading text.
Font style	Select the font style from the drop-down list.
Alignment	Select the heading text alignment from the drop-down list.
Left margin	Select the left margin value from the drop-down list.
Right margin	Select the right margin value from the drop-down list.
Switch to	Select to change the heading type. This will not change the font size, style, or color.

3. Select *OK* to apply your changes.

Text boxes

Text boxes can be added to content sections of the report template. A text box can also be added to the *Header Text* and footer sections if they contain no other elements.

When adding text to the report header or footer, you can only edit the content. Additional settings, such as color or font, are not available.

To add a text box:

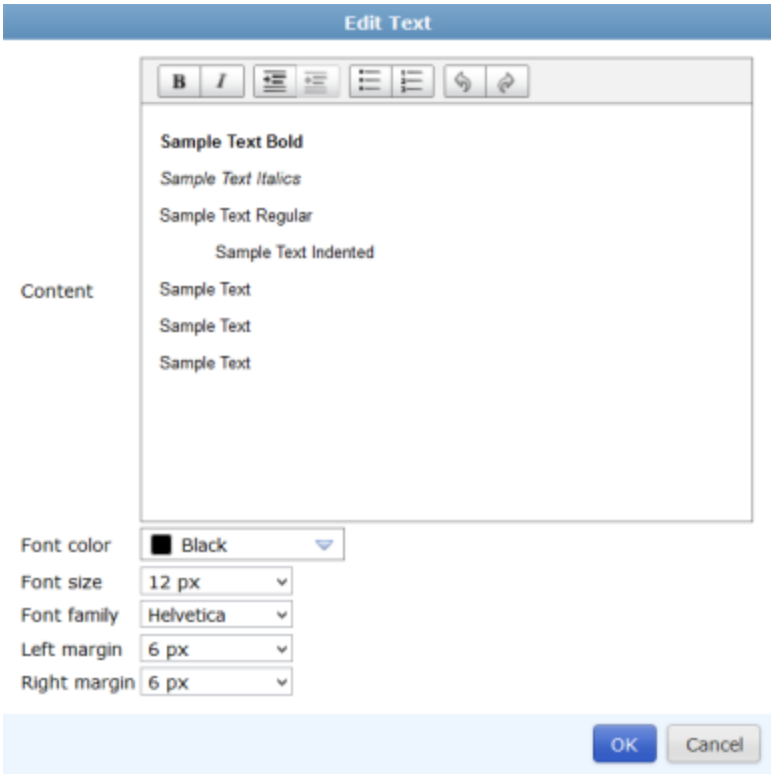
Click and drag the text icon from the template toolbar to the location in the section where you want to add text.

A single text box can be added to the *Header Text* Section and the footer section. Multiple text boxes can be added to content sections.

It is recommended that you edit the section prior to adding text elements as the section menu will override settings in an existing custom text section. See Sections on page 166.

To edit text:

1. Select the edit icon in the text box toolbar or double-click on the text box, to open the *Edit Text* dialog box.



2. Configure the following settings:

Content	Enter the text in this text field. You can change text elements in the text toolbar. The following options are available: bold, italics, indent, outdent, bulleted list, numbered list, undo, and redo. Use the right-click menu to cut, copy, paste, and delete content. You can also configure languages and the spell checker.
Font color	Select the font color from the drop-down list.
Font size	Select the font size from the drop-down list. The default size is 12 px.
Font family	Select the font family from the drop-down list.
Font style	Select the font style from the drop-down list.

Left margin	Select the left margin size from the drop-down list.
Right margin	Select the right margin size from the drop-down list.

The text field supports macros in XML format. See Macro library on page 180.

3. Select *OK* to finish editing the text.

Images

A single image can be added to the *Header Image* section. Multiple images can be added to content sections.

To add an image:

1. Click and drag the image icon to the location where you want to add the image. The *Choose a graphic* dialog box will open.
2. Select an image from the list, or select *Upload* to browse for an image on your computer.
3. Select *OK* to add the selected image to the report template. The image will appear in the location that you had selected in the template.

To edit an image:

1. Select the edit icon in the image toolbar or double-click on the image, to open the *Choose a graphic* dialog box.
2. Change the graphic as need, then select *OK*.

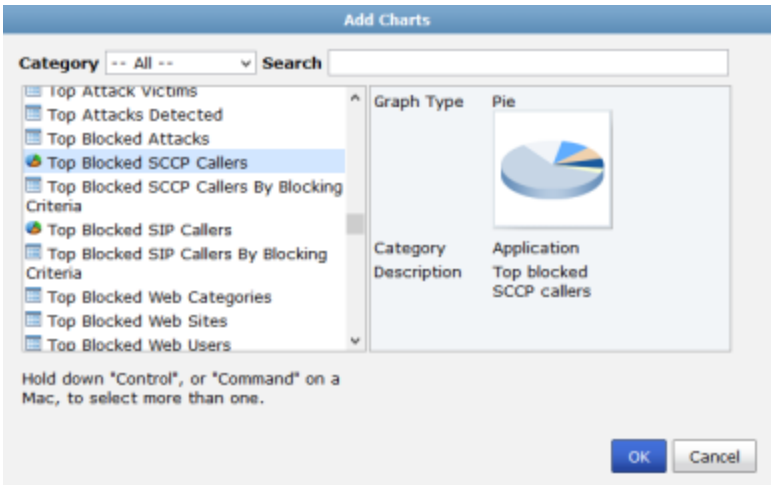
Charts

Chart elements can only be placed in content sections of the report template. The chart content can be filtered, and the chart content can be edited.

Predefined chart content cannot be changed. If attempting to edit a predefined chart, you will be prompted with a warning dialog box and given the option to clone the chart and make changes. The clone will replace the predefined chart in the report template.

To add a chart:

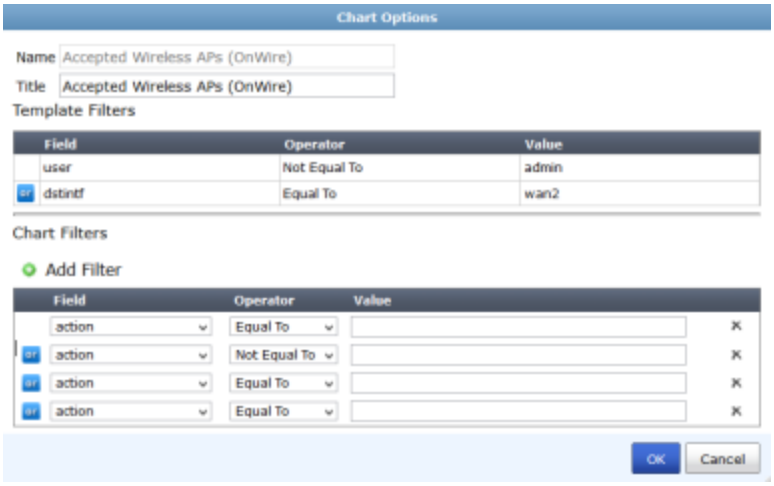
1. Click and drag the chart icon to the location where you want to add the chart. The *Add Charts* dialog box will open.



2. Find the chart that you would like to add in one of the following ways:
   - Browse the list of all the available the available charts.
   - Select the category of the chart you are looking for from the *Category* drop-down list, then browse the list of the charts in that category.
   - Search for the chart by entering all or part of the chart name into the *Search* field.
3. Select *OK* once you have found and selected the chart you would like to add.
   The chart's placeholder will appear in the location that you had selected in the template.

To add chart filters:

1. Select the chart options icon in the chart toolbar. The *Chart Options* dialog box will open.
   This page displays template filters and allows you to add chart filters.



2. Add charts filters to the chart as needed.
3. Select *OK* to apply the filters to the chart and return to the report layout page.

To edit a chart:

1. Select the edit icon in the chart toolbar or double-click on the chart.
2. If you are attempting to edit a predefined chart, a warning dialog box will open. Select *Copy and Edit* to continue editing a clone of the chart.

   The *Edit Chart* or *Clone Chart* (if editing a predefined chart) dialog box will open. See To edit a chart: on page 179 for more information on editing and cloning charts.
3. Select *OK* to apply your changes.

Breaks

Two types of breaks can be added to the content sections of a report template: line breaks, and page breaks. Breaks can not be edited.

To add a break:

Click and drag the line break or page break icon to the location in a content section in the report template where you want to add the break.

Chart library

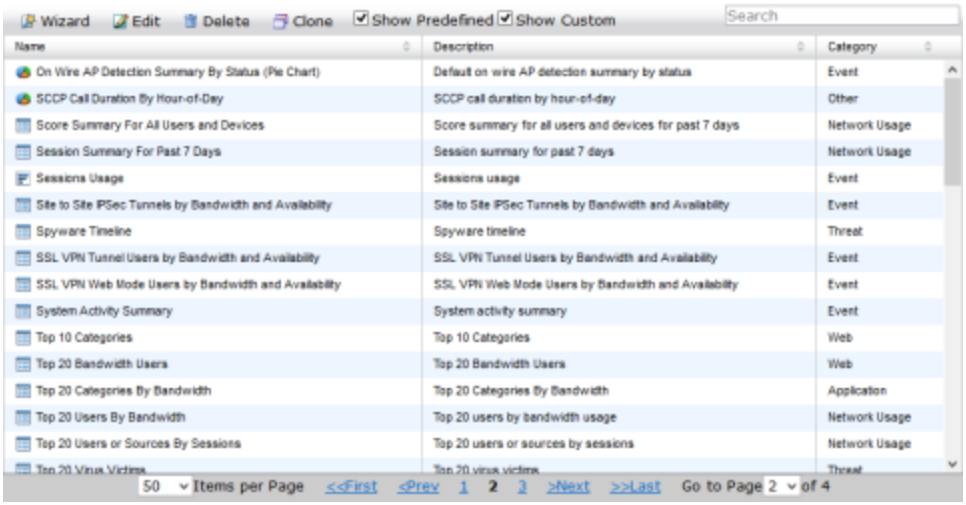
The FortiAnalyzer unit provides a selection of predefined charts. New charts can be created using the custom chart wizard, by cloning and editing an existing chart, or by using the advanced chart creation option. You can select to display predefined chart, custom charts, or both.

To view a listing of the available predefined charts, see Appendix B - Charts, Datasets, & Macros on page 206.

For advanced users, right-click the right content pane and select *Create New* to create SQL based charts. See To create a new chart: on page 177.

Charts are predefined to show specific information in an appropriate format, such as pie charts or tables. They are organized into categories, and can be added to, removed from, and organized in reports.

To view the chart library, go to *Reports* > *Chart Library*.



The following information is displayed:

Name	The name of the chart. Click the column header to sort entries in the table by name.
Description	The chart description. Click the column header to sort entries in the table by description.
Category	The chart category. Click the column header to sort entries in the table by category.
Pagination	Adjust the number of entries that are listed per page and browse through the pages.

The following options are available in the toolbar:

Wizard	Launch the custom chart wizard. This option is only available for FortiGate and FortiCarrier ADOMs. See Custom chart wizard on page 174.
Create New	Create a new chart. For FortiGate and FortiCarrier ADOMs, this option is only available from the right-click menu. See To create a new chart: on page 177.
Edit	Select to edit a chart. This option is only available for custom charts. See To edit a chart: on page 179.
View	Select to view chart details. This option is only available for predefined charts, as they cannot be edited.
Delete	Select to delete a chart. This option is only available for custom charts. See To delete charts: on page 180.
Clone	Select to clone an existing chart. See To clone a chart: on page 179.
Show Predefined	Select to display predefined charts.
Show Custom	Select to display custom charts.
Search	Enter a search term in the search field to find a specific chart.

Custom chart wizard

The custom chart wizard is a step by step guide to help you create custom charts. It is only available for FortiGate and FortiCarrier ADOMs.

To start the custom chart wizard, go to *Reports* > *Chart Library*, and select *Wizard* in the toolbar. Follow the steps in the chart wizard, outlined below, to create a custom chart.

Select the *Tutorial* icon on any of the wizard windows to view the online chart wizard video.

Step 1 of 3 - Choose data

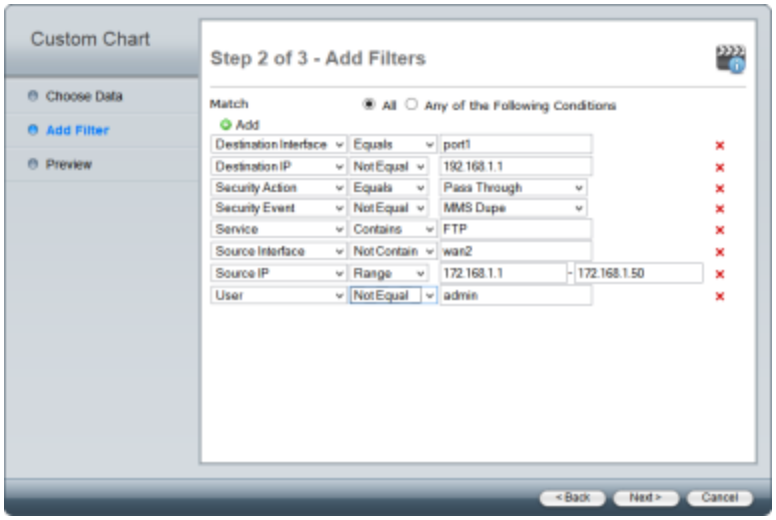
Configure the data that the custom chart will use.

Configure the following settings, then select *Next* to proceed to the next step:

Log Type	Select either *Traffic Log* or *Event Log*.
Group by	Select how the data are grouped. Depending on the chart type selected in step 3, this selection will relate to *Column 1* (Table), the *Y-axis* (Bar and Line graphs), or the *Legend* (Pie chart). See Step 3 of 3 - Preview on page 176. The available options will vary depending on the selected log type: • Traffic log: *Application Category, Application ID, Application Name, Attack, Destination Country, Destination Interface, Destination IP, Device Type, Source Interface, Source IP, Source SSID, User, Virus, VPN, VPN Type, Web Category*, or *Website (Hostname)*. • Event log: *VPN Tunnel*, or *Remote IP*.
Aggregate by	Select how the data is aggregated. Depending on the chart type selected in step 3, this selection will relate to *Column 2* (Table), the *X-axis* (Bar and Line graphs), or the *Value* (Pie chart). See Step 3 of 3 - Preview on page 176. The following options are available: *Duration*, *Received Bytes*, *Sent Bytes*, *Total Bytes*, *Total Sessions* or *Total Blocked Sessions* (Traffic log only).
Show	Select how much data to show in the chart from the drop-down list. One of the following: *Top 5*, *Top 10*, *Top 25*, *Top 50*, or *Top 100*.

Step 2 of 3 - Add filters

You can add one or more filters to the chart. These filters will be permanently saved to the dataset query.

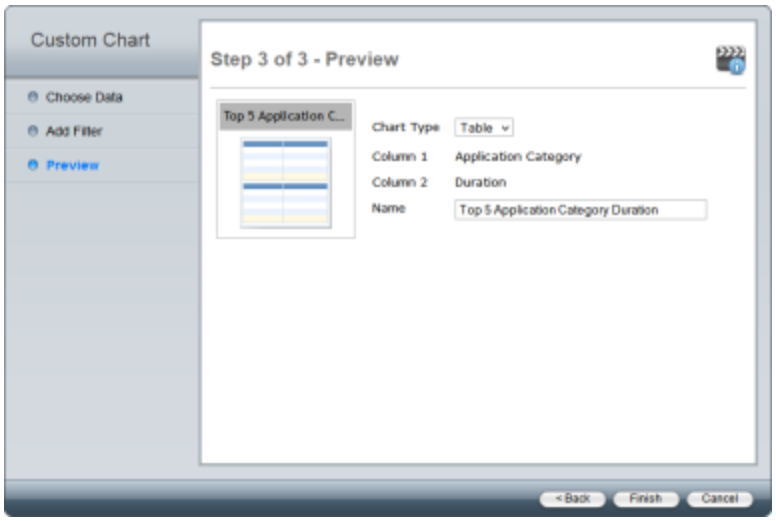


Configure the following settings:

Match		Select *All* to filter data based on all of the added conditions, or select *Any of the Following Conditions* to filter the data based on any one of the conditions.
Add		Select to add filters. For each filter, select the field, and operator from the drop-down lists, then enter or select the value as applicable. Filters vary based on device type. The available filters vary depending on the log type selected. Select the delete icon to remove a filter.
	Destination Interface	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
	Destination IP	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, and *Range*. If *Range* is selected, enter the starting and ending IP address in the value fields.
	Security Action	This filter is available for traffic logs only. The available operators are: *Equals* and *Not Equal*. The value is always *Pass Through*.
	Security Event	Select *Equals or Not Equal* from the second drop-down list. Select one of the below options from the third drop-down list. This filter is available for traffic logs only. The value can be one of the following: *Analytics*, *Application Control*, *AV Error*, *Banned Word*, *Command Block*, *DLP*, *File Filter*, *General Mail Log*, *HTML Script Virus*, *IPS*, *MIME Fragmented*, *MMS Checksum*, *MMS Dupe*, *MMS Endpoint*, *MMS Flood*, *MAC Quarantine*, *Oversize*, *Script Filter*, *Spam Filter*, *SSH Block*, *SSH Log*, *Switching Protocols*, *Virus*, *VOIP*, *Web Content*, *Web Filter*, or *Worm*.
	Service	This filter is available for both traffic and event logs. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
	Source Interface	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
	Source IP	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, and *Range*. If *Range* is selected, enter the starting and ending IP address in the value fields.
	User	This filter is available for both traffic and event logs. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.

Step 3 of 3 - Preview

The preview page allows you to select the chart type and rename the custom chart.



Configure the following settings:

Chart Type	Select the chart type in the drop-down list; one of the following: *Bar*, *Line*, *Pie*, or *Table*. Depending on the chart settings configured in the previous two steps, the available options may be limited.
Column 1 / Y-axis / Legend	Displays the *Group by* selection. See Group by on page 175. The field varies depending on the chart type.
Column 2 / X-axis / Value	Displays the *Aggregate by* selection. See Aggregate by on page 175. The field varies depending on the chart type.
Name	Displays the default name of the custom chart. This field can be edited.

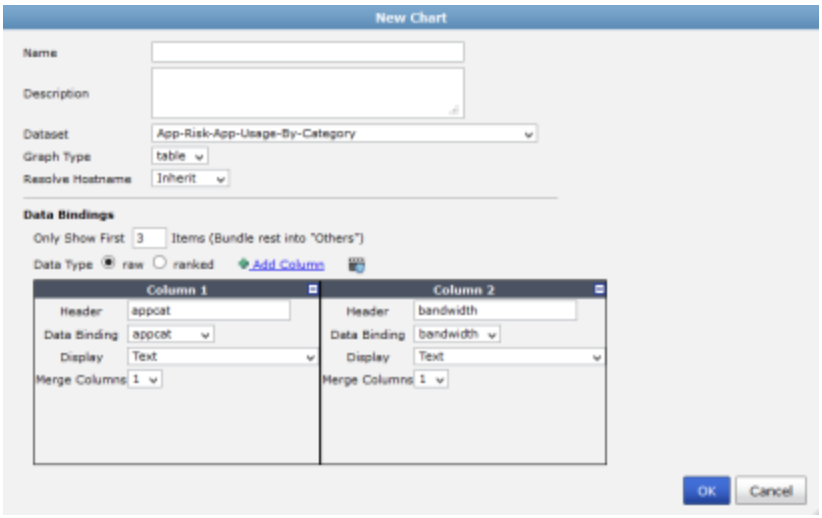
Select *Finish* to finish the wizard and create the custom chart. The custom chart will be added to the chart table and will be available for use in report templates.

Managing charts

Predefined charts can be viewed and cloned. Custom charts can be created, edited, cloned, and deleted.

To create a new chart:

1. In the chart library:
   - If you are creating a chart in a FortiGate or FortiCarrier ADOM: right-click in the content pane and select *Create New*.
   - If you are creating a chart in any other ADOM: select *Create New* in the toolbar. The *New Chart* dialog box opens.



2. Select the *Tutorial* icon to view the online chart creation video.
3. Enter the required information for the new chart.

Name	Enter a name for the chart.
Description	Enter a description of the chart.
Dataset	Select a dataset from the drop-down list. See Dataset on page 185 for more information. The options will vary based on device type.
Graph Type	Select a graph type from the drop-down list; one of: *table*, *bar*, *pie*, or *line*. This selection will affect the rest of the available selections.
Line Subtype	Select one of the following options: *basic*, *stacked*, or *back-to-back*. This option is only available when creating a line graph.
Resolve Hostname	Select to resolve the hostname. Select one of the following: *Inherit*, *Enabled*, or *Disabled*.
Data Bindings	The data bindings vary depending on the chart type selected.
bar, pie, or line graphs	
X-Axis	• *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. • *Only Show First*: Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the *Others* category. • *Overwrite label*: Enter a label for the axis.

	Y-Axis	• *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. • *Overwrite label*: Enter a label for the axis. • *Group by*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. This option is only available when creating a bar graph.
	Order By	Select to order by the X-Axis or Y-Axis. This option is only available when creating a line or bar graph.
table		
	Only Show First Items	Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the *Others* category. This option is available for all columns when *Data Type* is set to *raw*. When *Data Type* is set to ranked, this option is available in *Column 1*.
	Data Type	Select either *ranked* or *raw*.
	Add Column	Select add column icon to add a column.
	Columns	Up to fifteen columns can be added. The following column settings must be set: • *Header*: Enter header information. • *Data Binding*: Select a value from the drop-down list. The options vary depending on the selected dataset. • *Display*: Select a value from the drop-down list. • *Merge Columns*: Select a value from the drop-down list. This option is only available when *Data Type* is *raw*. If applicable, enter a *Merge Header*. • *Order by this column*: Select to order the table by this column. This option is only available in *Column 1* when *Data Type* is *ranked*.

4. Select *OK* to create the new chart.

To clone a chart:

1. In the chart library, select the chart that you would like to clone and select *Clone* from either the toolbar or right-click menu. The *Clone Chart* dialog box opens.
2. Edit the information as needed, then select *OK* to clone the chart.

To edit a chart:

1. In the chart library, double-click on the custom chart you need to edit, or select the chart then select *Edit* from either the toolbar or right-click menu. The *Edit Chart* dialog box opens.
2. Edit the information as required, then select *OK* to finish editing the chart.

Predefined charts cannot be edited, the information is read-only. A predefined chart can be cloned, and changes can then be made to said clone.

To delete charts:

1. In the chart library, select the custom chart or charts that you would like to delete and select *Delete* from either the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the chart or charts.

Predefined charts cannot be deleted.

Macro library

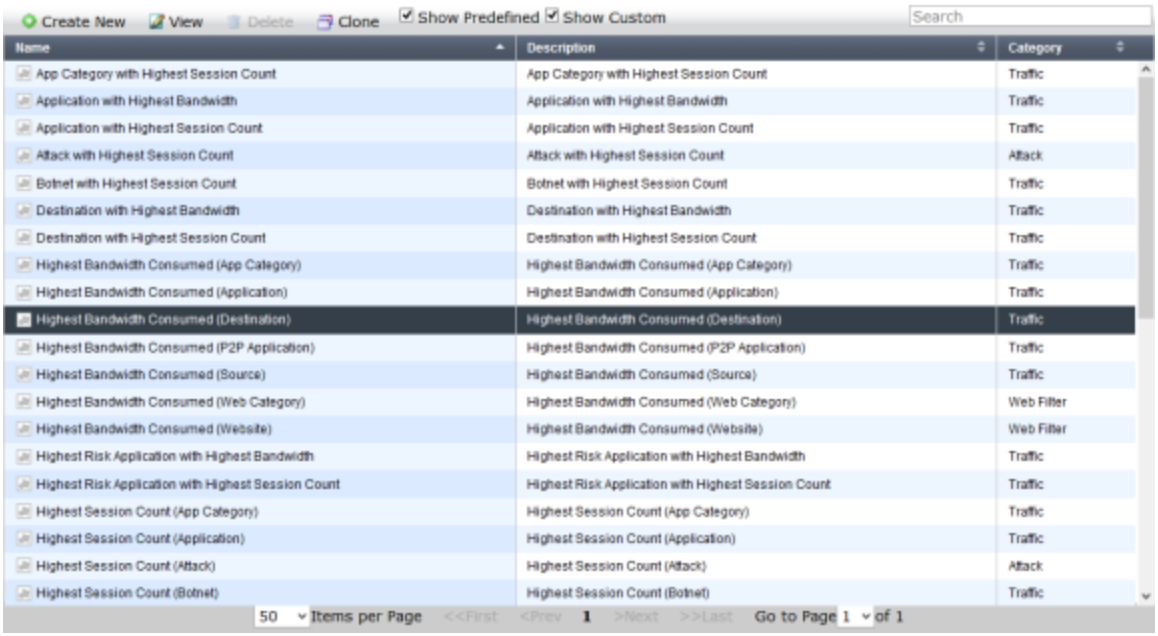
The FortiAnalyzer unit provides a selection of predefined macros. You can create new macros and clone existing macros. You can select to display predefined macros, custom macros, or both.

To view a listing of the available predefined macros, see Appendix B - Charts, Datasets, & Macros on page 206.

Macros are predefined to use specific datasets and queries. They are organized into categories, and can be added to, removed from, and organized in reports.

Macros are currently supported in FortiGate and FortiCarrier ADOMs only.

To view the macro library, go to *Reports* > *Macro Library*.



The following information is available:

Name	The name of the macro.

Description	The macro description.
Category	The macro category.
Pagination	Adjust the number of entries that are listed per page and browse through the pages.

The following options are available in the toolbar:

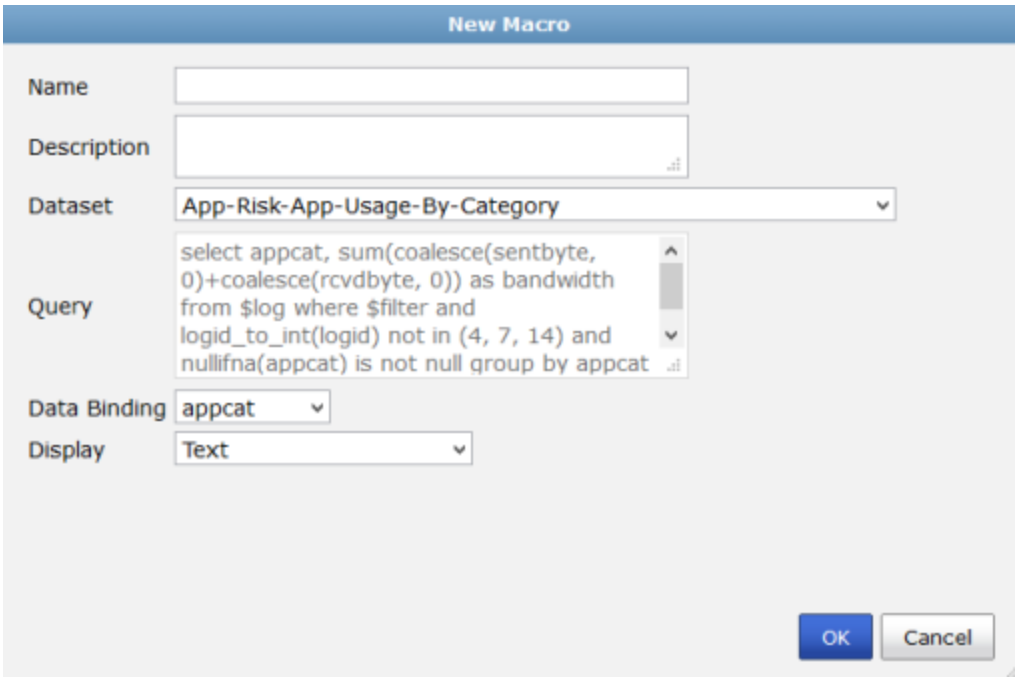
Create New	Create a new macro. This option is only available from the right-click menu.
Edit	Select to edit a macro. This option is only available for custom macros.
View	Select to view macro details. This option is only available for predefined macros, as they cannot be edited.
Delete	Select to delete a macro. This option is only available for custom macros.
Clone	Select to clone an existing macro.
Show Predefined	Select to display predefined macros.
Show Custom	Select to display custom macros.
Search	Enter a search term in the search field to find a specific macros.

Managing macros

Predefined macros can be viewed and cloned. Custom macros can be created, edited, cloned, and deleted. You can insert macros into text elements in the report layout.

To create a new macro:

1. In the macro library, select *Create New* in the toolbar or right-click in the content pane and select *Create New*. The *New Macro* dialog box opens.



2. Enter the required information for the new macro.

Name	Enter a name for the macro.
Description	Enter a description of the macro.
Dataset	Select a dataset from the drop-down list. See Dataset on page 185 for more information. The options will vary based on device type.
Query	Displays the query statement for the dataset selected.
Data Binding	The data bindings vary depending on the dataset selected. Select a data binding from the drop-down list.
Display	Select a value from the drop-down list.

3. Select *OK* to create the new macro.

To clone a macro:

1. In the macro library, select the macro that you would like to clone and select *Clone* from either the toolbar or right-click menu. The *Clone Macro* dialog box opens.
2. Edit the information as needed, then select *OK* to clone the macro.

To view a predefined macro:

1. In the macro library, double-click on the predefined macro you would like to view, or select the macro then select *View* from either the toolbar or right-click menu. The *View Macro* dialog box opens. All fields are read-only.
2. Select *Close* when you are finished.

To edit a macro:

1. In the macro library, double-click on the custom macro you need to edit, or select the macro then select *Edit* from either the toolbar or right-click menu. The *Edit Macro* dialog box opens.
2. Edit the information as required, then select *OK* to finish editing the macro.

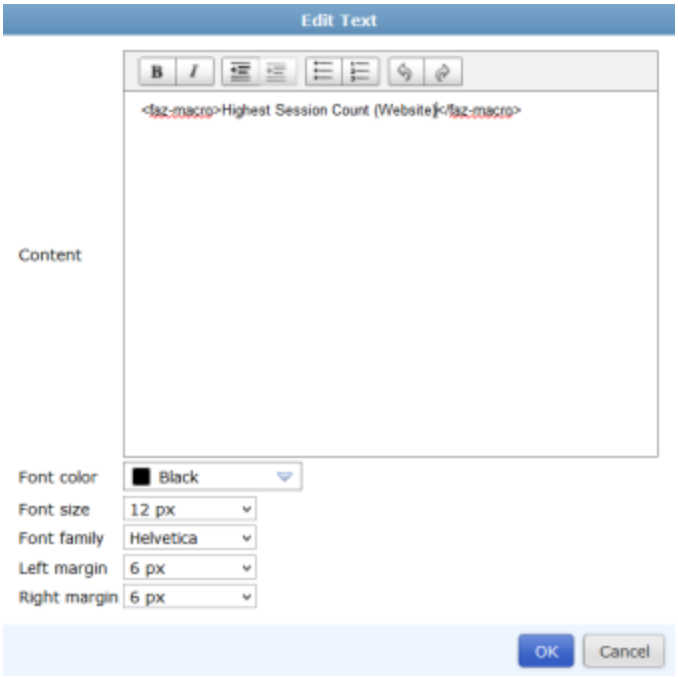
To delete macros:

1. In the macro library, select the custom macro or macros that you would like to delete and select *Delete* from either the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the macro or macros.

Predefined macros cannot be deleted.

To use macros:

1. In a report, select the *Layout* tab.
2. Drag and drop the text element into a section.
3. Select the edit icon, in the section toolbar. The *Edit Text* dialog box opens.

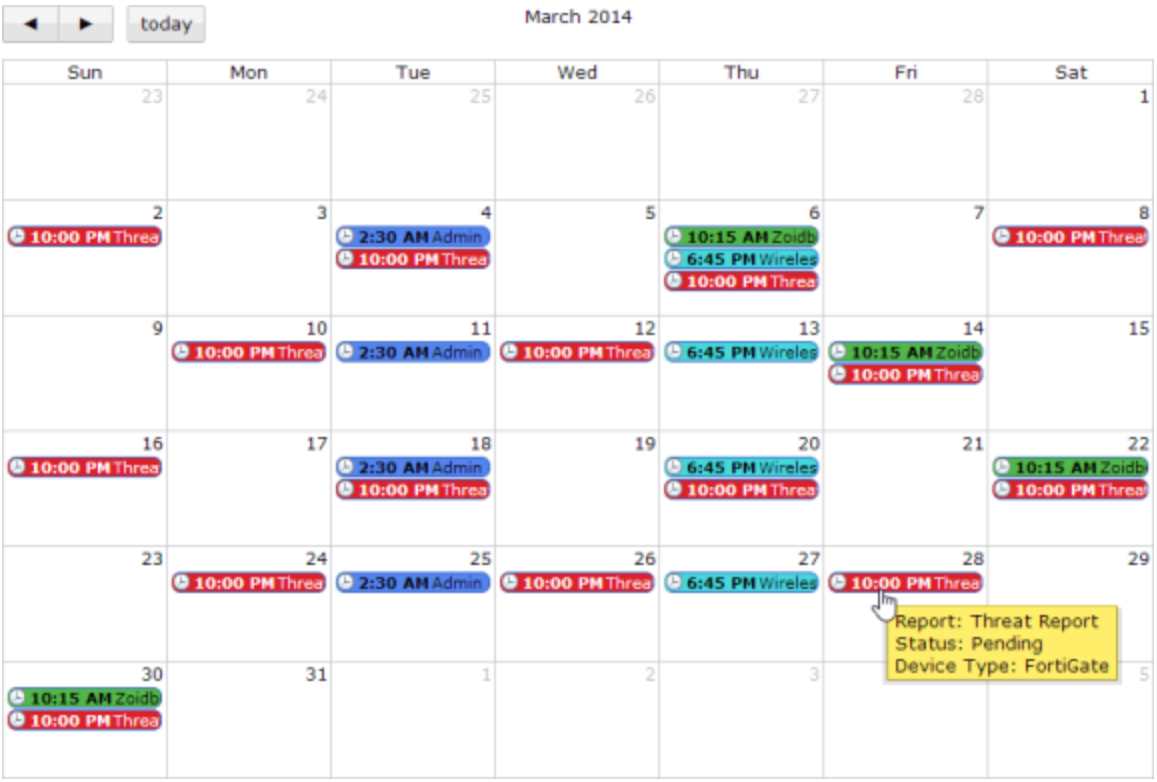


4. Enter the name of the macro in the XML open `<faz-macro>` and close `</faz-macro>` tags.
   For example, `<faz-macro>Highest Session Count (Website)</faz-macro>`.
5. Select *OK* to save the text element.
6. Select *Save* to save the report template change.

Report calendar

The report calendar provides an overview of scheduled reports. You can view all reports scheduled for the selected month. From the calendar page, you can edit and disable upcoming reports, and delete or download completed reports.

To view the report calendar, go to *Reports* > *Report Calendar*.



Hovering the mouse cursor over a scheduled report on the calendar opens a notification box that shows the report's name and status, as well as the device type.

Selecting the left and right arrows at the top of the calendar page will adjust the month that is shown. Select *Today* to return to the current month.

To edit a report schedule:

1. Right-click on the scheduled report in the report calendar and select *Edit*. The *Edit Report* window will open.
2. Edit the report settings as required, then select *Apply* to apply the changes.

To disable a scheduled report:

1. Right-click the scheduled report and select *Disable* from the right-click menu.
2. In the confirmation box, select *OK*.

   Disabling a report will remove all scheduled instances of the report from the report calendar. Completed reports will remain in the report calendar.

To delete a scheduled report:

1. Right-click the scheduled report that you would like to delete and select *Delete*. Only scheduled reports that have already been run can be deleted.
2. Select *OK* in the confirmation dialog box to delete the scheduled report.

To download a report:

1. Right-click the scheduled report that you would like to download and select *Download*. Only scheduled reports that have already been run can be downloaded.
2. Depending on your web browser and management computer settings, save the file to your computer, or open the file in an applicable program.

   Reports are downloaded as PDF files.

Advanced

The advanced menu allows you to view, configure and test datasets, create output profiles, and manage report languages.

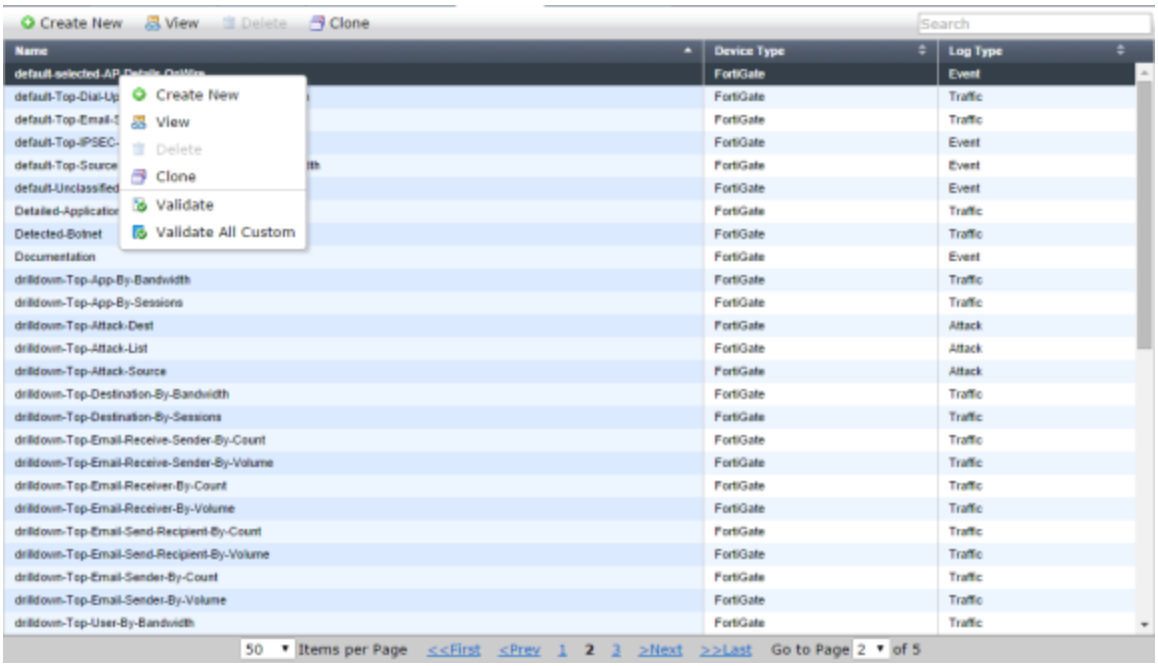
Dataset

FortiAnalyzer datasets are collections of log files from monitored devices. Reports are generated based on these datasets.

To view a listing of the available predefined datasets, see Appendix B - Charts, Datasets, & Macros on page 206.

Predefined datasets for each supported device type are provided, and new datasets can be created and configured. Both predefined and custom datasets can be cloned, but only custom datasets can be deleted. You can also view the SQL query for a dataset, and test the query against specific devices or all devices.

To view and configure datasets, go to *Reports* > *Advanced* > *Dataset* in the tree menu.



The following information is displayed:

Name	The name of the dataset.
Device Type	The device type that the dataset applies to.
Log Type	The type of log that the dataset applies to.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.

The following options are available in the toolbar:

Create New	Select to create a new dataset.
View	Select to view the dataset. View is only available for pre-defined datasets.
Edit	Select to edit an existing dataset.
Delete	Select to delete a dataset.
Clone	Select to clone an existing dataset.
Search	Use the search field to find a specific dataset.

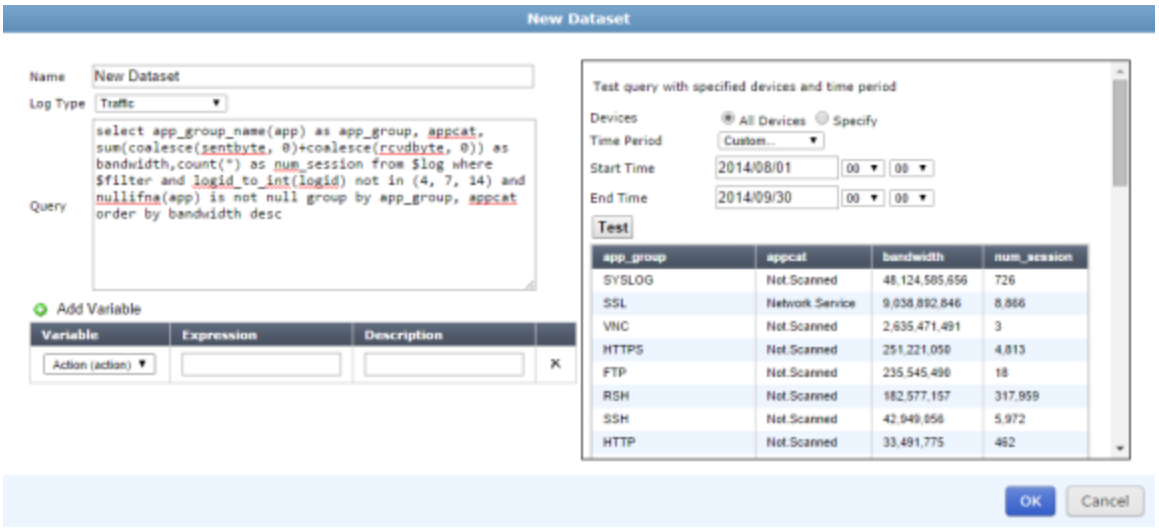
The following options are available in the right-click menu:

Create New	Select to create a new dataset.

View	Select a dataset, right-click, and select *View* to view the dataset selected. View is only available for pre-defined datasets.
Delete	Select a custom dataset, right-click, and select *Delete* to remove the custom dataset. You cannot delete pre-defined datasets.
Clone	Select a custom dataset, right-click, and select *Clone* to clone the dataset.
Validate	Select a custom dataset, right-click, and select *Validate* to validate the selected dataset. A validation result dialog box will be displayed with the results.
Validate All Custom	Right-click in the right pane and select *Validate All Custom* to validate all custom datasets. A validation result dialog box will be displayed with the results.

To create a new dataset:

1. In the dataset list, either select *Create New* from the toolbar, or right-click in the dataset list and select *Create New* from the pop-up menu. The *New Dataset* dialog box opens.



2. Enter the required information for the new dataset.

Name	Enter a name for the dataset.

Log Type	Select a log type from the drop-down list. • The following log types are available for FortiGate: *Application Control*, *Attack*, *DLP Archive*, *DLP*, *Email Filter*, *Event*, *Traffic*, *Virus*, *Web Filter*, and *Network Scan*. • The following log types are available for FortiMail: *Email Filter*, *Event*, *History*, and *Virus*. • The following log types are available for FortiWeb: *Attack*, *Event*, and *Traffic*. • The following log types are available for FortiCache: *Application Control*, *Attack*, *DLP Archive*, *DLP*, *Email Filter*, *Event*, *Traffic*, *Virus*, *Web Filter*, and *Network Scan*.
Query	Enter the SQL query used for the dataset.
Add Variable	Select the add variable icon to add a variable, expression, and description information.
Test query with specified devices and time period	
Devices	Select *All Devices* or *Specify* to select specific devices to run the SQL query against. Use the add device icon to add multiple devices to the query.
Time Period	Use the drop-down list to select a time period. When selecting Other, enter the start date, time, end date, and time.
Test	Select Test to test the SQL query before saving the dataset configuration.

3. Test the query to ensure that the dataset functions as expected, then select *OK* to create the new dataset.

To clone a dataset:

1. In the dataset list, either select a dataset then select *Clone* from the toolbar, or right-click on the dataset then select *Clone* from the pop-up menu. The *New Dataset* dialog box opens.
2. Edit the information as required, then test the query to ensure that the dataset functions as expected.
3. Select *OK* to create a new, cloned dataset.

To edit a dataset:

1. In the dataset list double-click on the dataset, or select the dataset then select *Edit* from the toolbar or right-click menu. The *Edit Dataset* dialog box opens.
2. Edit the information as required, then test the query to ensure that the dataset functions as expected.
3. Select *OK* to finish editing the dataset.

Predefined datasets cannot be edited, the information is read-only. You can view the SQL query and variables used in the dataset and test against specific devices.

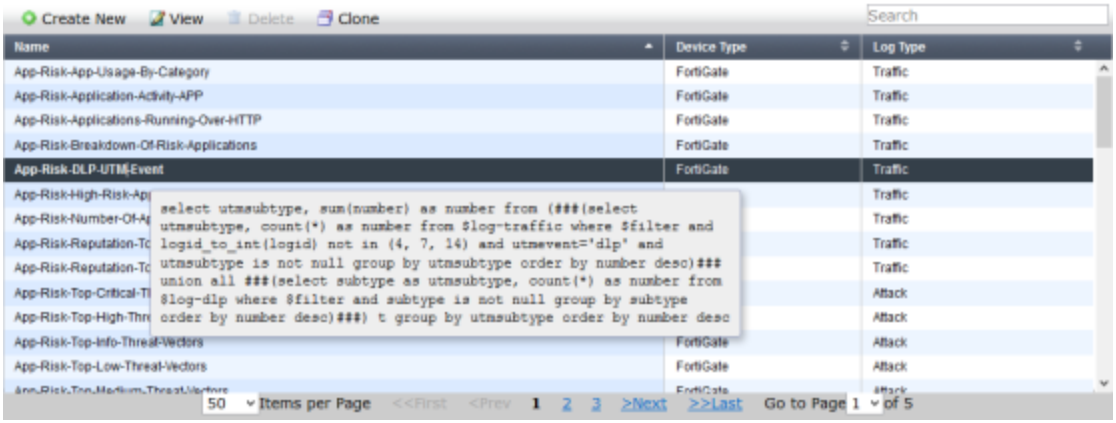
To delete datasets:

1. Select the dataset or datasets that you would like to delete, then select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected dataset or datasets.

Predefined datasets cannot be deleted, the information is read-only.

To view the SQL query for an existing dataset:

Hover the mouse cursor over one of the datasets in the dataset list. The SQL query is displayed in a persistent pop-up dialog box.



To validate a custom dataset:

1. Select a custom dataset, right-click, and select *Validate* to validate the selected dataset. A validation result dialog box will be displayed with the results.
2. If errors exist, select to edit the dataset to fix the errors as identified in the validation dialog box.

Output profile

Output profiles allow you to define email addresses to which generated reports are sent, and provides an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report; see Reports on page 156.

To view and manage output profiles, go to *Reports* > *Advanced* > *Output Profile*.

You must configure a mail server before you can configure an output profile. See Mail server on page 109.

To create a new output profile:

1. In the output profile list, select *Create New* from either the toolbar or right-click menu. The *New Output Profile* dialog box opens.

2. Enter the following information:

Name	Enter a name for the new output profile.
Description	Enter a description for the output profile (optional).
Email Generated Reports	Enable email generated reports.
Subject	Enter a subject for the report email.
Body	Enter body text for the report email.
Email Recipients	Select the email server from the drop-down list and enter to and from email addresses. Select *Add New* to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading the reports to a server.
Report Format	Select the report format or formats. The options include *PDF* and *HTML*.
Server Type	Select *FTP*, *SFTP*, or *SCP* from the drop-down list.
Server	Enter the server IP address.

	User	Enter the username.
	Password	Enter the password.
	Directory	Specify the directory where the report will be saved.
	Delete file(s) after uploading	Select to delete the report after it has been uploaded to the selected.

3. Select *OK* to create the new output profile.

To edit an output profile:

1. In the output profile list, double-click on the output profile that you would like to edit, or select the output profile and select *Edit* from the toolbar or right-click menu. The *Edit Output Profile* dialog box opens.
2. Edit the information as required, then select *OK* to apply your changes.

To delete output profiles:

1. In the output profile list, select the output profile or profiles that you would like to delete, then select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected output profile or profiles.

Language

The language of the reports can be specified when creating a report (see Advanced settings tab on page 160). New languages can be added, and the name and description of the languages can be changed. The predefined languages cannot be edited.

To view and manage report languages, go to *Reports* > *Advanced* > *Language*.

The available, pre-configured report languages include:

English (default report language)	Portuguese
French	Simplified Chinese
Japanese	Spanish
Korean	Traditional Chinese

To add a language:

1. In the report language list, select *Create New* from the toolbar or right-click menu. The *New Language* dialog box opens.
2. Enter a name and description for the language in the requisite fields.
3. Select *OK* to add the language.

Adding a new language does not create that language. It only adds a placeholder for that language that contains the language name and description.

To edit a language:

1. In the report language list, double-click on the language that you would like to edit, or select the language and select *Edit* from the toolbar or right-click menu. The *Edit Language* dialog box opens.
2. Edit the information as required, then select *OK* to apply your changes.

To delete languages:

1. In the report language list, select the language or languages that you would like to delete and select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected language or languages.

Predefined languages cannot be edited or deleted; the information is read-only.

Language translation files

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

Appendix A - Report Templates

FortiAnalyzer includes preconfigured reports and report templates for FortiGate, FortiMail, FortiCache, and FortiWeb log devices. These report templates can be used as is, or you can clone and edit the templates. You can also create new reports and report templates that can be customized to your requirements.

Predefined report templates are identified by a blue report icon and custom report templates are identified by a green report icon. When a schedule has been enabled, the schedule icon will appear to the left of the report template name.

FortiGate reports

The following tables list the default report templates and the charts they contain.

Report Template	Charts
Admin and System Events Report	Admin Login • Login Summary • Login Summary By Date • List of Failed Logins System Events • Events by Severity • Events by Date • Critical Severity Events • High Security Events • Medium Security Events

Report Template	Charts
Application and Risk Analysis	Top Application Users By Bandwidth • Top Users By Bandwidth Top Application Users By Session • Top User Sources By Sessions Client Reputation • Top Users By Reputation Scores • Top Devices By Reputation Scores Application Usage By Category • Top 10 Application Categories by Bandwidth Usage • Application Categories By Bandwidth Usage Applications Detected by Risk Behavior • Number of Applications by Risk Behavior • High Risk Applications Key Applications Crossing The Network • Key Applications Crossing The Network Applications Running Over HTTP • Top Applications Running Over HTTP Top Web Categories Visited By Network Users • Top Web Categories By Sessions • Top Web Categories By Sessions/Bandwidth Top Web Sites Visited By Network Users • Top Web Domains By Visits Top Destination Countries By Browsing Time • Top Destination Countries By Browsing Time Top Web Sites By Browsing Time • Top Web Sites By Browsing Time Top Threats Crossing The Network • Top Threats Crossing The Network • Top Critical Threats Crossing The Network • Top High Threats Crossing The Network • Top Medium Threats Crossing The Network • Top Low Threats Crossing The Network • Top Info Threats Crossing The Network Top 20 Viruses Crossing The Network • Top Viruses By Name Top Virus Victims • Top Virus Victims • Malwares Discovered • Application Vulnerabilities Discovered Data Loss Prevention Events • Top Data Loss Prevention Events

Report Template	Charts
Bandwidth and Applications Report	Traffic Summary • Bandwidth Summary • Sessions Summary • Traffic Statistics Application Traffic • Top 30 Applications by Bandwidth and Sessions • Application Categories by Bandwidth Users • Top 30 Users by Bandwidth and Sessions • Active Users Destinations • Top 30 Destinations by Bandwidth and Sessions
Client Reputation	Summary for Users and Devices • Score Summary for All Users/Devices • Top Users by Reputation Scores • Top Users With Increased Scores for Last 2 Periods • Number of Incidents for All Users/Devices • Top Devices by Reputation Scores • Top Devices with Increased Scores for Last 2 Periods

Report Template	Charts
Detailed Application Usage and Risk	Risk 5: Botnet • Session History Graph • Application Usage List Risk 5: Proxy Avoidance • Session History Graph • Application Usage List Risk 4: Peer To Peer • Session History Graph • Application Usage List Risk 4: Remote Access • Session History Graph • Application Usage List Risk 3: Instant Messaging • Session History Graph • Application Usage List Risk 3: Email • Session History Graph • Application Usage List Risk 3: Storage and Backup • Session History Graph • Application Usage List Risk 2: General Access Categories • Session History Graph • Application Usage List Risk 1: Reduced Risk Categories • Session History Graph • Application Usage List • Browser Usage Breakdown • Application Usage List
Email Report	• Top Senders by Number of Emails • Top Recipients by Number of Emails • Top Senders by Combined Email Size • Top Recipients by Combined Email Size

Report Template	Charts
IPS Report	Summary • Intrusions By Severity • Intrusions Timeline • Intrusions By Types Intrusions Detected • Critical Severity Intrusions • High Severity Intrusions • Medium Severity Intrusions • Low Severity Intrusions • Intrusion Victims • Intrusion Sources • Intrusions Blocked • Intrusions Monitored • Attacks Over HTTP/HTTPS

Report Template	Charts
Security Analysis	Bandwidth and Applications • Traffic Bandwidth • Number of Sessions • Top Applications by Bandwidth • Top Applications by Sessions • Top Users by Bandwidth • Top Users by Sessions • Top Destination by Bandwidth • Top Destination by Sessions • DHCP Summary • Top Wifi Client by Bandwidth • Traffic History by Number of Active Users Web Usage • Top 20 Most Active Users • Top 20 Most Visited Categories • Top 50 Most Visited Sites • Top 10 Online Users • Top 10 Categories • Top 50 Sites By Browsing Time • Top 20 Bandwidth Users • Top 20 Categories By Bandwidth • Top 50 Sites (and Category) by Bandwidth • Top 20 Most Blocked Users • Top 20 Most Blocked Categories • Top 50 Most Blocked Sites Emails • Top Senders by Number of Emails • Top Recipients by Number of Emails • Top Senders by Combined Email Size • Top Recipients by Combined Email Size Threats • Malware Detected • Malware Victims • Malware Source • Botnet Detected • Botnet Victims • Botnet C&C • Intrusions Detected • Intrusion Victims • Intrusion Sources

Report Template	Charts
Security Analysis (cont'd)	VPN Usage • VPN Traffic Usage Trend • VPN User Logins • Authenticated Logins • Failed Login Attempts • Top Dial-up VPN Users • Top Sources of SSL VPN Tunnels by Bandwidth • Top SSL VPN Tunnel Users by Bandwidth • Top SSL VPN Web Mode Users by Bandwidth • Top SSL Users by Duration • Top Users of IPsec VPN Dial-up Tunnel by Bandwidth • Top Site-to-Site IPsec Tunnels by Bandwidth • Top Dial-up IPsec Tunnels by Bandwidth • Top Dial-up IPsec Users by Bandwidth • Top Dial-Up IPsec Users by Duration Admin Login and System Events • Login Summary • Login Summary By Date • List of Failed Logins • Events by Severity • Events By Date • Critical Severity Events • High Severity Events • Medium Severity Events

Report Template	Charts
Threat Report	Malware • Malware Detected • Malware Victims • Malware Source • Malware Timeline Botnets • Botnet Detected • Botnet Victims • Botnet C&C • Botnet Timeline Intrusions • Intrusions Detected • Intrusion Victims • Intrusion Sources • Intrusions By Severity • Intrusions Blocked • Intrusion Timeline
User Report	• Top 5 Users By Bandwidth
User Security Analysis	• Top Blocked Web Sites • Top Allowed Web Sites • Top Blocked Web Categories • Top Allowed Web Categories • Top Attacks • Top Attacks with High Severity • Top Viruses • Top Virus Receivers Over Email • Count of Spam Activity by Hour of Day • Top Spam Sources

Report Template	Charts
VPN Report	Summary • VPN Traffic Usage Trend • VPN User Logins • Authenticated Logins • Failed Login Attempts • Top Dial-Up VPN Users SSL VPN • Top Sources of SSL VPN Tunnels by Bandwidth • Top SSL VPN Tunnel Users by Bandwidth • Top SSL VPN Web Mode Users by Bandwidth • Top SSL VPN Users by Duration IPsec VPN • Top Users of IPsec VPN Dial-Up Tunnel by Bandwidth • Top Site-to-Site IPsec Tunnels By Bandwidth • Top Dial-up IPsec Tunnels by Bandwidth • Top Dial-up IPsec Users by Bandwidth • Top Dial-up IPsec Users by Duration
Web Usage Report	Web Usage Summary • Requests Summary • Browsing Time Summary • Bandwidth Summary Web Activity • Top 20 Most Active Users • Top 20 Most Visited Categories • Top 50 Most Visited Sites Web Browsing • Top 10 Online Users • Top 10 Categories • Top 50 Sites By Browsing Time Internet Bandwidth Usage • Top 20 Bandwidth Users • Top 20 Categories By Bandwidth • Top 50 Sites (and Category) by Bandwidth Most Blocked • Top 20 Most Blocked Users • Top 20 Most Blocked Categories • Top 50 Most Blocked Sites

Report Template	Charts
WiFi Network Summary	Network Summary • Overall Data Transferred • Number of Distinct Clients Wireless Usage and Clients • Top APs by Usage • SSID Usage • Top Application by Usage • Top Operating Systems by Usage • Top Device Type by Usage • Top APs by Number of Clients • Top SSID by Number of Clients • Top Clients by Usage • Top Operating Systems by Number of WiFi Clients • Top Device Type by Number of Clients
Wireless PCI Compliance	Summary • Managed AP Summary • AP Detection Summary (OnWire) • AP Detection Summary (OffWire) • Unclassified AP Summary (OnWire + OffWire) OnWire APs • Rogue Wireless APs • Suppressed Wireless APs • Accepted Wireless APs • Unclassified Wireless APs OffWire APs • Rogue Wireless APs • Suppressed Wireless APs • Accepted Wireless APs • Unclassified Wireless APs

The following report template can be found in the *Application* folder.

Report Template	Charts
Applications - Top 20 Categories and Applications (Bandwidth)	Top 20 Categories and Applications (Bandwidth)
Applications - Top 20 Categories and Applications (Session)	Top 20 Categories and Applications (Session)
Applications - Top Allowed and Blocked with Timestamps	Top 500 Allowed Applications by Bandwidth Top 500 Blocked Applications by Session

The following report templates can be found in the *Detailed User Report* folder.

Report Template	Charts
User Detailed Browsing Log	Detailed Browsing Log
User Top 500 Websites by Bandwidth	Top 500 Websites by Bandwidth
User Top 500 Websites by Session	Top 500 Websites by Session

The following report templates can be found in the *Web* report folder.

Report Template	Charts
Hourly Website Hits	Hourly Website Hits
Top 20 Category And Websites (Bandwidth)	Top 20 Category And Websites (Bandwidth)
Top 20 Category And Websites (Hits)	Top 20 Category And Websites (Hits)
Top 500 Sessions by Bandwidth	Top 500 Sessions by Bandwidth

FortiMail reports

The following table lists report templates exclusive to FortiMail devices.

Report Template	Charts
FortiMail Analysis Report	Statistics • Average Size of Mails • Total Size of Mails • Number of Mail Connections • Number of Mails • Total Message Delay • Total Message Transmission Delay • Top IP Policy • Top Recipient Policy • Top Access List Incoming Filtering • Top Spammed Domains • Top Spammed Users • Top Classifiers by Hour • Top Disposition Classifiers • Top Subjects
FortiMail Default Report	• Top10 Client IP • Top10 Senders • Top10 Virus Senders • Top10 Local Users • Top10 Recipients • Top10 Virus Recipients

FortiWeb report

The following table lists report templates exclusive to FortiWeb devices.

Report Template	Charts
FortiWeb Default Report	• Top Sources of Attacks • Top Sources • Top Event Categories • Top Login Events by User • Top Attack Destinations • Top Destinations • Top Event Types

FortiCache report

The following table lists report templates exclusive to FortiCache devices.

Report Template	Charts
FortiCache Default Report	• Top 20 Websites by Bandwidth Savings • Top 20 Websites by Cache Rate • Top 20 Websites by Response Time Improvement

Appendix B - Charts, Datasets, & Macros

FortiGate

Predefined charts

The following table lists the predefined charts for FortiGate.

Display Name	Description	Category
Active Traffic Users	List of active traffic users	Network Usage
Admin Login Summary by Date	Administrator login summary by date	Event
Adware Timeline	Adware timeline	Threat
Application Bandwidth Usage	Application bandwidth usage details	Network Usage
Application Category with Highest Session Count	Application category with the highest session count	
Application Risk Distribution	Application risk distribution	Application
Application with Highest Bandwidth	Application with the highest bandwidth usage	
Application with Highest Session Count	Applications with the highest session count	
Applications Running over HTTP	Applications running over HTTP protocol	Application
Attack Summary	Intrusion events summary	Threat
Attack with Highest Session Count	Attack with highest session count	
Attacks Over HTTP/HTTPs	Intrusions over HTTP or HTTPs	Threat
Bandwidth Summary	Traffic bandwidth usage summary	Network Usage
Botnet Timeline	Botnet timeline	Network Usage
Botnet Victims	Botnet victims	Network Usage

Display Name	Description	Category
Botnet with Highest Session Count	Botnet with the highest session count	
Browsing Time Summary	Browsing time summary	Web
CPU Session Usage	CPU session usage	Event
CPU Usage	CPU usage	Event
Destination with Highest Bandwidth	Destination with the highest bandwidth usage	
Destination with Highest Session Count	Destination with the highest session count	
Detailed Web Browsing Log	Detailed browsing log of web	Traffic
Detected Botnets	Detected botnets	Network Usage
Detected OS Count	Detected operating system count	Traffic
Distribution of SIP Calls by Duration	Distribution of SIP calls by duration	Other
Drilldown Top 20 Applications by Bandwidth	Drilldown top 20 applications by bandwidth usage	Application
Drilldown Top 20 Applications by Bandwidth Bar Chart	Drilldown top 20 applications by bandwidth usage bar chart	Application
Drilldown Top 20 Applications by Sessions	Drilldown top 20 applications by session count	Application
Drilldown Top 20 Applications by Sessions Bar Chart	Drilldown top 20 applications by session count bar chart	Application
Drilldown Top 20 Attack Destination	Drilldown top 20 attack destinations	Threat
Drilldown Top 20 Attack List	Drilldown top 20 attack list	Threat
Drilldown Top 20 Destination by Bandwidth	Drilldown top 20 destination by bandwidth usage	Network Usage
Drilldown Top 20 Destination by Sessions	Drilldown top 20 destination by session count	Network Usage
Drilldown Top 20 Email Receive Sender by Count	Drilldown top 20 email-receive senders by count	Email

Display Name	Description	Category
Drilldown Top 20 Email Receive Sender by Volume	Drilldown top 20 email-receive senders by volume	Email
Drilldown Top 20 Email Recipient by Count	Drilldown top 20 email recipients by count	Email
Drilldown Top 20 Email Recipient by Volume	Drilldown top 20 email recipients by volume	Email
Drilldown Top 20 Email Send Recipient by Count	Drilldown top 20 email-send recipients by count	Email
Drilldown Top 20 Email Send Recipient by Volume	Drilldown top 20 Email-Send recipients by volume	Email
Drilldown Top 20 Email Sender by Count	Drilldown top 20 email senders by count	Email
Drilldown Top 20 Email Sender by Volume	Drilldown top 20 email senders by volume	Email
Drilldown Top 20 User by Bandwidth	Drilldown top 20 users by bandwidth	Network Usage
Drilldown Top 20 User by Bandwidth Bar Chart	Drilldown top 20 users by bandwidth usage bar chart	Network Usage
Drilldown Top 20 User by Sessions	Drilldown top 20 users by session count	Network Usage
Drilldown Top 20 User by Sessions Bar Chart	Drilldown top 20 users by session count bar chart	Network Usage
Drilldown Top 20 Viruses	Drilldown top 20 viruses	Threat
Drilldown Top 20 Web User by Visits	Drilldown top 20 web users by visits	Web
Drilldown Top 20 Web User by Visits Bar Chart	Drilldown top 20 web users by visits bar chart	Web
Drilldown Top 20 Website by Requests	Drilldown top 20 web sites by requests	Web
Drilldown Top 20 Website by Requests Bar Chart	Drilldown top 20 web sites by requests bar chart	Web
Drilldown Top Attack Source	Drilldown top attack sources	Threat
Drilldown Virus Details	Drilldown virus details	Threat

Display Name	Description	Category
Highest Bandwidth by Application	Highest bandwidth consumed by application	
Highest Bandwidth by Application Category	Highest bandwidth consumed by application category	
Highest Bandwidth by Destination	Highest bandwidth consumed by destination	
Highest Bandwidth by P2P Application	Highest bandwidth consumed by P2P application	
Highest Bandwidth by Source	Highest bandwidth consumed by source	
Highest Bandwidth by Web Category	Highest bandwidth consumed by website category	
Highest Bandwidth by Website	Highest bandwidth consumed by website	
Highest Risk Application with Highest Bandwidth	Highest risk application with the highest bandwidth usage	
Highest Risk Application with Highest Session Count	Highest risk application with the highest session count	
Highest Session Count by Application	Highest session count by application	
Highest Session Count by Application Category	Highest session count by application category	
Highest Session Count by Attack	Highest session count by attack	
Highest Session Count by Botnet	Highest session count by botnet	
Highest Session Count by Destination	Highest session count by destination	
Highest Session Count by Highest Severity Attack	Highest session count by highest severity attack	
Highest Session Count by P2P Application	Highest session count by P2P application	
Highest Session Count by Source	Highest session count by source	

Display Name	Description	Category
Highest Session Count by Virus	Highest session count by virus	
Highest Session Count by Web Category	Highest session count by website category	
Highest Session Count by Website	Highest session count by website	
Highest Severity Attack with Highest Session Count	Highest severity attack with the highest session count	
Hourly Category and Website Hits	Hourly category and website hits	Traffic
Intrusions Timeline	Intrusions timeline by severity	Threat
Managed AP Summary Pie Chart	Managed wireless access point summary by status pie chart	Event
Memory Usage	Memory usage	Event
Number of Applications by Risk Behaviour	Number of applications by risk behaviour	Application
Number of Distinct WiFi Clients	Number of distinct WiFi clients	Network Usage
Number of SCCP Call Registrations by Hour-of-Day	Number of SCCP call registrations by hour of day	Other
Number of SCCP Calls by Status	Number of SCCP calls by status	Other
Number of SIP Call Registrations by Hour-of-Day	Number of SIP call registrations by hour of day	Other
Number of SIP Calls by Status	Number of SIP calls by status	Other
Off-Wire Rogue APs	Rogue off-wire wireless access points	WiFi
P2P Application with Highest Bandwidth	P2P applications with the highest bandwidth usage	
P2P Application with Highest Session Count	P2P applications with the highest session count	
SCCP Call Duration by Hour-of-Day	SCCP call duration by hour of day	Other
Session History Graph	Session history graph	Event
Session Summary	Session summary	Network Usage

Display Name	Description	Category
Session Usage	Session usage	Event
Source with Highest Bandwidth	Source with the highest bandwidth usage	
Source with Highest Session Count	Source with the highest session count	
Spyware Timeline	Spyware timeline	Threat
System Events Summary by Date	System events summary by date	Event
Threat Incident Summary	Number of incidents for all users and devices	Network Usage
Threat Score Summary	Threat score summary for all users and devices	Network Usage
Top 5 Attacks by Severity	Top 5 attacks by severity	Threat
Top 5 IPS Events by Severity	Top 5 intrusion protection events by severity	Threat
Top 5 System Events by Severity	Top 5 system events summary by severity	Event
Top 5 Users by Bandwidth	Top 5 users by bandwidth usage	Network Usage
Top 15 Destination Countries by Browsing Time	Top 15 destination countries by browsing time	Web
Top 15 Websites by Browsing Time	Top 15 websites by browsing time	Network Usage
Top 20 Admin Login Summary	Top 20 login summary of administrator	Event
Top 20 Allowed Web Categories	Top 20 allowed web filtering categories	Web
Top 20 Application Categories by Bandwidth	Top 20 application categories by bandwidth usage	Application
Top 20 Bandwidth Users	Top 20 web users by bandwidth users	Web
Top 20 Blocked Intrusions	Top 20 blocked intrusions	Threat

Display Name	Description	Category
Top 20 Blocked Web Categories	Top 20 blocked web filtering categories	Web
Top 20 Category and Applications by Bandwidth	Top 20 category and applications by bandwidth usage	Traffic
Top 20 Category and Applications by Sessions	Top 20 category and applications by session count	Traffic
Top 20 Category and Websites by Bandwidth	Top 20 category and websites by bandwidth usage	Traffic
Top 20 Category and Websites by Sessions	Top 20 category and websites by session count	Traffic
Top 20 Critical Severity Intrusions	Top 20 critical severity intrusions	Threat
Top 20 Failed Admin Logins	Top 20 failed logins of administrator	Event
Top 20 High Risk Applications	Top 20 high risk applications	Application
Top 20 High Severity Intrusions	Top 20 high severity intrusions	Threat
Top 20 Intrusion Sources	Top 20 intrusion sources	Threat
Top 20 Intrusion Victims	Top 20 intrusion victims	Threat
Top 20 Intrusions by Types	Top 20 intrusions by types	Threat
Top 20 Low Severity Intrusions	Top 20 low severity intrusions	Threat
Top 20 Medium Severity Intrusions	Top 20 medium severity intrusions	Threat
Top 20 Monitored Intrusions	Top 20 monitored intrusions	Threat
Top 20 Users by Bandwidth	Top 20 users by bandwidth usage	Network Usage
Top 20 Users or Sources by Sessions	Top 20 users or sources by session count	Network Usage
Top 20 Virus Victims	Top 20 virus victims	Threat
Top 20 Viruses	Top 20 viruses detected	Threat
Top 20 Web Categories by Bandwidth and Sessions	Top 20 web filtering categories by bandwidth usage and session count	Web

Display Name	Description	Category
Top 20 Web Domains by Visits	Top 20 visited web domains by number of visits	Web
Top 20 Web Users by Requests	Top 20 web users by number of requests	Web
Top 30 Application Categories by Bandwidth	Top 30 application categories by bandwidth usage	Application
Top 30 Applications by Bandwidth and Sessions	Top 30 applications by bandwidth usage and session count	Application
Top 30 Destinations by Bandwidth and Sessions	Top 30 destinations by bandwidth usage and session count	Application
Top 30 Key Applications	Top 30 key applications crossing the network	Application
Top 30 Users by Bandwidth and Sessions	Top 30 users by bandwidth usage and session count	Network Usage
Top 50 Allowed Websites	Top 50 allowed websites by number of requests	Web
Top 50 Allowed Websites by Requests	Top 50 allowed websites by number of requests	Web
Top 50 Websites and Category by Bandwidth	Top 50 websites and web filtering categories by bandwidth usage	Web
Top 50 Websites by Browsing Time	Top 50 websites by browsing time	Web
Top 100 Critical Severity System Events	Top 100 critical severity system events	Event
Top 100 High Severity System Events	Top 100 high severity system events	Event
Top 100 Medium Severity System Events	Top 100 medium severity system events	Event
Top 100 Off-Wire Accepted APs	Top 100 off-wire accepted wireless access points	WiFi
Top 100 Off-Wire Suppressed APs	Top 100 suppressed off-wire wireless access points	WiFi

Display Name	Description	Category
Top 100 Off-Wire Unclassified APs	Top 100 unclassified off-wire wireless access points	WiFi
Top 100 On-Wire Accepted APs	Top 100 on-wire accepted wireless access points	WiFi
Top 100 On-Wire Rogue APs	Top 100 rogue on-wire wireless access points	WiFi
Top 100 On-Wire Suppressed APs	Top 100 suppressed on-wire wireless access points	WiFi
Top 100 On-Wire Unclassified APs	Top 100 unclassified on-wire wireless access points	WiFi
Top 100 WiFi Client Details	Top 100 details of client event of wireless access point	Event
Top 500 Allowed Applications by Bandwidth	Top 500 allowed applications by bandwidth usage	Traffic
Top 500 Blocked Applications by Sessions	Top 500 blocked applications by session count	Traffic
Top 500 Websites by Bandwidth	Top 500 website sessions by bandwidth usage	Traffic
Top Adware	Top 10 adware	Threat
Top Adware Sources	Top 10 adware sources	Threat
Top Adware Victims	Top 10 adware victims	Threat
Top Allowed Websites by Bandwidth	Top 10 allowed websites by bandwidth usage	Web
Top Application Categories Bandwidth	Top 10 application categories by bandwidth usage	Application
Top Application Categories by Bandwidth	Top 10 application categories by bandwidth usage	Application
Top Application Vulnerabilities	Top 10 application vulnerabilities discovered	Other
Top Applications by Bandwidth	Top 10 applications by bandwidth usage	Application

Display Name	Description	Category
Top Applications by Sessions	Top 10 applications by session count	Application
Top Applications by WiFi Traffic	Top 10 applications by WiFi bandwidth usage	Application
Top APs by Bandwidth	Top 10 wireless access points by WiFi bandwidth usage	Network Usage
Top APs by WiFi Clients	Top 10 wireless access points by number of clients via WiFi	Network Usage
Top Attack Sources	Top 10 attack sources	Threat
Top Attack Victims	Top 10 attack victims	Threat
Top Attacks	Top 10 intrusions	Threat
Top Authenticated VPN Logins	Top 10 authenticated VPN logins	Event
Top Blocked Attacks	Top 10 blocked intrusions	Threat
Top Blocked SCCP Callers	Top 10 blocked SCCP callers	Application
Top Blocked SIP Callers	Top 10 blocked SIP callers	Application
Top Blocked Web Users	Top 10 blocked web users	Web
Top Blocked Websites	Top 10 blocked websites by number of requests	Web
Top Blocked Websites and Categories	Top 10 blocked web filtering websites and categories by number of requests	Web
Top Botnet Infected Hosts	Top 10 botnet infected hosts	Network Usage
Top Botnet Sources	Top 10 botnet sources	Network Usage
Top Botnets by Sources	Top 10 botnets by sources	Network Usage
Top Critical Severity IPS Events	Top 10 critical severity intrusion protection events	Threat
Top Destination Countries by Browsing Time	Top 10 destination countries by browsing time	Web
Top Destinations by Bandwidth	Top 10 destination addresses by bandwidth usage	Network Usage

Display Name	Description	Category
Top Destinations by Sessions	Top 10 destination addresses by session count	Network Usage
Top Device Types by WiFi Clients	Top 10 device types by number of clients via WiFi	Network Usage
Top Device Types by WiFi Traffic	Top 10 device types by WiFi bandwidth usage	Network Usage
Top Devices by Increased Threat Scores	Top 10 devices by increased threat scores for last two periods	Network Usage
Top Devices by Threat Score	Top 10 devices by threat score in risk	Network Usage
Top Devices by Threat Scores	Top 10 devices by threat scores	Network Usage
Top DHCP Summary by Interfaces	Top 10 DHCP summary by interfaces	Event
Top Dial-up IPsec Tunnels by Bandwidth	Top 10 dial-up IPsec VPN tunnels by bandwidth usage	Network Usage
Top Dial-up IPsec Users by Bandwidth	Top 10 users of dial-up IPsec VPN by bandwidth usage	Network Usage
Top Dial-up IPsec Users by Bandwidth and Availability	Top 10 users of dial-up IPsec VPN tunnel by bandwidth usage and availability	Event
Top Dial-up IPsec Users by Duration	Top 10 users of dial-up IPsec VPN by duration	VPN
Top Dial-up VPN Users by Duration	Top 10 users of dial-up SSL and IPsec VPN by duration	VPN
Top DLP Events	Top 10 data leak prevention events	DLP
Top Email Recipients	Top 10 recipients by number of emails	Email
Top Email Senders	Top 10 senders by number of emails	Email
Top Failed VPN Logins	Top 10 failed VPN login attempts	Event
Top High Severity IPS Events	Top 10 high severity intrusion protection events	Threat

Display Name	Description	Category
Top Informational Severity IPS Events	Top 10 informational severity intrusion protection events	Threat
Top IPsec Dial-up User by Bandwidth	Top 10 users of IPsec VPN dial-up tunnel by bandwidth usage	Network Usage
Top Low Severity IPS Events	Top 10 low severity intrusion protection events	Threat
Top Malware	Top malware detected by malware type	Threat
Top Malware Sources	Top 10 malware sources by host name or IP address	Threat
Top Managed AP Summary	Top 10 managed wireless access point summary by status	Event
Top Medium Severity IPS Events	Top 10 medium severity intrusion protection events	Threat
Top Off-Wire AP Details	Top 10 details of off-wire wireless access point	Event
Top Off-Wire AP Summary	Top 10 off-wire wireless access point detection summary by status	Event
Top Off-Wire AP Summary Pie Chart	Top 10 off-wire wireless access point detection summary by status pie chart	Event
Top On-Wire AP Details	Top 10 details of on-wire wireless access point	Event
Top On-Wire AP Summary	Top 10 on-wire wireless access point detection summary by status	Event
Top On-Wire AP Summary Pie Chart	Top 10 on-wire wireless access point detection summary by status pie chart	Event
Top OS by WiFi Clients	Top 10 operating systems by number of clients via WiFi	Network Usage
Top OS by WiFi Traffic	Top 10 operating systems by WiFi bandwidth usage	Network Usage

Display Name	Description	Category
Top Recipients by Aggregated Email Size	Top 10 recipients by aggregated email size	Email
Top Search Phrases	Top 10 search filtering phrases	Web
Top Senders by Aggregated Email Size	Top 10 senders by aggregated email size	Email
Top Site-to-Site IPsec Tunnels by Bandwidth	Top 10 site-to-site IPsec VPN tunnels by bandwidth usage	Network Usage
Top Site-to-Site IPsec Tunnels by Bandwidth and Availability	Top 10 Site-to-Site IPsec tunnels by bandwidth usage and availability	Event
Top Spyware	Top 10 spyware	Threat
Top Spyware Sources	Top 10 spyware sources	Threat
Top Spyware Victims	Top 10 spyware victims	Threat
Top SSIDs by Bandwidth	Top 10 SSIDs by WiFi bandwidth usage	Network Usage
Top SSIDs by WiFi Clients	Top 10 SSIDs by number of clients via WiFi	Network Usage
Top SSL Tunnel Users by Bandwidth	Top 10 users of SSL VPN tunnel by bandwidth usage	VPN
Top SSL Tunnel Users by Bandwidth and Availability	Top 10 users of SSL VPN tunnel by bandwidth usage and availability	Event
Top SSL Users by Duration	Top 10 users of SSL VPN web portal and tunnel by duration	VPN
Top SSL VPN Sources by Bandwidth	Top 10 users of SSL VPN tunnel by bandwidth usage	VPN
Top SSL Web Portal Users by Bandwidth	Top 10 users of SSL VPN web portal by bandwidth usage	VPN
Top SSL Web Portal Users by Bandwidth and Availability	Top 10 users of SSL web portal by bandwidth usage and availability	Event
Top Unclassified AP Summary	Top 10 unclassified wireless access point summary by status	Event

Display Name	Description	Category
Top Users Browsing Time	Top 10 users by estimated web browsing time	Network Usage
Top Users by Bandwidth	Top 10 users by bandwidth usage	Network Usage
Top Users by Browsing Time	Top 10 users by estimated web browsing time	Network Usage
Top Users by Increased Threat Scores	Top 10 users by increased threat scores for last 2 periods	Network Usage
Top Users by Sessions	Top 10 users by session count	Network Usage
Top Users by Threat Scores	Top 10 users by threat scores	Network Usage
Top Users Threat Score	Top 10 users by threat score	Network Usage
Top Video Streaming Applications and Websites by Bandwidth	Top 10 video streaming applications and websites by bandwidth usage	Web
Top Video Streaming Websites by Bandwidth	Top 10 video streaming websites of web filter by bandwidth usage	Web
Top Virus Victims	Top virus victims	Threat
Top Viruses	Top 10 viruses detected	Threat
Top Web Categories by Bandwidth and Sessions	Top 10 web filtering categories by bandwidth usage and session count	Web
Top Web Categories by Browsing Time	Top 10 web filtering categories by browsing time	Web
Top Web Users by Allowed Requests	Top 10 web users by number of allowed requests	Web
Top Web Users by Bandwidth	Top 10 web users by bandwidth usage	Web
Top Web Users by Blocked Requests	Top 10 web users by number of blocked requests	Web
Top Web Users by Browsing Time	Top 10 web users by browsing time	Web
Top WiFi Clients Bandwidth	Top 10 WiFi clients by bandwidth usage	Network Usage

Display Name	Description	Category
Top WiFi Clients by Bandwidth	Top 10 clients by WiFi bandwidth usage	Network Usage
Total Number of Attacks	Total number of attacks detected	
Total Number of Botnet Events	Total number of botnet events	
Total Number of Viruses	Total number of viruses detected	
Traffic History	Traffic history by number of active users	Network Usage
Traffic Statistics	Top 10 traffic statistics summary	Application
Unclassified AP Summary Pie Chart	Unclassified wireless access point summary by status pie chart	Event
User Details	User Details	
User Drilldown Count Spam Activity by Hour Of Day	User drilldown count of spam activity by hour of day	Email
User Drilldown Top Allowed Web Categories	User drilldown top 10 allowed web categories	Web
User Drilldown Top Allowed Web Sites by Requests	User drilldown top 10 allowed web sites by requests	Web
User Drilldown Top Attacks	User drilldown top 10 attacks	Threat
User Drilldown Top Attacks High Severity	User drilldown top 10 attacks high severity	Threat
User Drilldown Top Blocked Web Categories	User drilldown top 10 bloacked web categories	Web
User Drilldown Top Blocked Web Sites by Requests	User drilldown top 10 blocked web sites by requests	Web
User Drilldown Top Spam Sources	User drilldown top 10 spam sources	Email
User Drilldown Top Virus by Name	User drilldown top 10 virus by name	Threat
User Drilldown Top Virus Receivers Over Email	User Drilldown top 10 virus receivers over email	Threat
User Top 500 Websites by Bandwidth	Top 500 user visted websites by bandwidth usage	Traffic

Display Name	Description	Category
User Top 500 Websites by Sessions	Top 500 user visted websites by session count	Traffic
UTM Drilldown Email Receivers Summary	UTM drilldown email receivers summary	Email
UTM Drilldown Email Senders Summary	UTM drilldown email senders summary	Email
UTM Drilldown No.1 Traffic Summary	UTM drilldown number 1 traffic summary	Network Usage
UTM Drilldown Top 5 Applications by Bandwidth	UTM drilldown top 5 applications by bandwidth	Application
UTM Drilldown Top 5 Applications by Sessions	UTM drilldown top 5 applications by sessions	Application
UTM Drilldown Top 5 Email Recipients by Bandwidth	UTM drilldown top 5 email recipients by bandwidth	Email
UTM Drilldown Top 5 Email Senders by Bandwidth	UTM drilldown top 5 email senders by bandwidth	Email
UTM Drilldown Top 5 User Destination	UTM drilldown top 5 user destinations	Network Usage
UTM Drilldown Top 20 Attacks	UTM drilldown top 20 attacks by name	Threat
UTM Drilldown Top 20 Virus by Name	UTM drilldown top 20 viruses by name	Threat
UTM Drilldown Top 20 Vulnerability	Top 20 vulnerabilities by name	Other
UTM Drilldown Top Allowed Websites by Requests	UTM drilldown top 10 allowed sites by request	Web
UTM Drilldown Top Blocked Websites by Requests	UTM drilldown top 10 blocked sites by request	Web
Virus Timeline	Virus timeline	Threat
Virus with Highest Session Count	Virus with the highest session count	
Viruses Discovered	Viruses discovered	Network Usage
VPN Logins	List of VPN user logins	Event

Display Name	Description	Category
VPN Traffic Usage Trend	Bandwidth usage trend for VPN traffic	Event
Web Activity Summary	Web activity summary by number of requests	Web
Web Category with Highest Bandwidth	Web filtering category with the highest bandwidth usage	
Web Category with Highest Session Count	Web filtering category with the highest session count	
Website with Highest Bandwidth	Website with the highest bandwidth usage	
Website with Highest Session Count	Website with the highest session count	
WiFi Traffic Bandwidth	Overall WiFi traffic bandwidth usage	Network Usage

Predefined datasets

The following table lists the predefined datasets for FortiGate.

ID/Name	Description	Log Type
traffic-bandwidth-timeline	Traffic bandwidth timeline	traffic
number-of-session-timeline	Number of session timeline	traffic
Top-Users-By-Bandwidth	Top users by bandwidth usage	traffic
Top-App-By-Bandwidth	Top applications by bandwidth usage	traffic
Top-User-Source-By-Sessions	Top user source by session count	traffic
Top-User-By-Sessions	Top user by session count	traffic
Top-App-By-Sessions	Top applications by session count	traffic
Top-Destinations-By-Bandwidth	Top destinations by bandwidth usage	traffic
Top-Destinations-By-Sessions	Top destinations by session count	traffic
event-Top-DHCP-Summary	Event top dhcp summary	event

ID/Name	Description	Log Type
traffic-Top-WiFi-Client-By-Bandwidth	Traffic top WiFi client by bandwidth usage	traffic
Traffic-History-By-Active-User	Traffic history by active user	traffic
utm-Top-Allowed-Web-Sites-By-Request	UTM top allowed web sites by request	traffic
utm-Top-Blocked-Web-Sites-By-Request	UTM top blocked web sites by request	traffic
utm-Top-Web-Users-By-Request	UTM top web users by request	traffic
utm-Top-Allowed-Websites-By-Bandwidth	UTM top allowed websites by bandwidth usage	traffic
utm-Top-Blocked-Web-Users	UTM top blocked web users	traffic
utm-Top-Web-Users-By-Bandwidth	UTM top web users by bandwidth usage	traffic
utm-Top-Video-Streaming-Websites-By-Bandwidth	UTM top video streaming websites by bandwidth usage	traffic
default-Top-Email-Senders-By-Count	Default top email senders by count	traffic
default-Email-Top-Receivers-By-Count	Default email top receivers by count	traffic
default-Email-Top-Senders-By-Bandwidth	Default email top senders by bandwidth usage	traffic
default-Email-Top-Receivers-By-Bandwidth	Default email top receivers by bandwidth usage	traffic
utm-Top-Virus	UTM top virus	traffic
utm-Top-Virus-User	UTM top virus user	traffic
utm-Top-Attack-Source	UTM top attack source	attack
utm-Top-Attack-Dest	UTM top attack dest	attack
vpn-Top-Static-IPSEC-Tunnels-By-Bandwidth	Top static IPsec tunnels by bandwidth usage	event
vpn-Top-SSL-VPN-Tunnel-Users-By-Bandwidth	Top SSL VPN tunnel users by bandwidth usage	event
vpn-Top-SSL-VPN-Web-Mode-Users-By-Bandwidth	Top SSL VPN web mode users by bandwidth usage	event
vpn-Top-SSL-VPN-Users-By-Bandwidth	Top SSL VPN users by bandwidth usage	event

ID/Name	Description	Log Type
vpn-Top-SSL-VPN-Users-By-Duration	Top SSL VPN users by duration	event
vpn-Top-Dial-Up-IPSEC-Tunnels-By-Bandwidth	Top dial up IPsec tunnels by bandwidth usage	event
vpn-Top-Dial-Up-IPSEC-Users-By-Bandwidth	Top dial up IPsec users by bandwidth usage	event
vpn-Top-Dial-Up-IPSEC-Users-By-Duration	Top dial up IPsec users by duration	event
vpn-Top-Dial-Up-VPN-Users-By-Duration	Top dial up VPN users by duration	event
vpn-Traffic-Usage-Trend-VPN	VPN traffic usage trend	event
vpn-User-Login-history	VPN user login history	event
vpn-Authenticated-Logins	VPN authenticated logins	event
vpn-Failed-Logins	VPN failed logins	event
vpn-Top-S2S-IPSEC-Tunnels-By-Bandwidth-and-Avail	Top S2S IPsec tunnels by bandwidth usage and avail	event
vpn-Top-Dialup-IPSEC-Users-By-Bandwidth-and-Avail	Top dialup IPsec users by bandwidth usage and avail	event
vpn-Top-SSL-Tunnel-Users-By-Bandwidth-and-Avail	Top SSL tunnel users by bandwidth usage and avail	event
vpn-Top-SSL-Web-Users-By-Bandwidth-and-Avail	Top SSL web users by bandwidth usage and avail	event
event-Admin-Login-Summary	Event admin login summary	event
event-Admin-Login-Summary-By-Date	Event admin login summary by date	event
event-Admin-Failed-Login-Summary	Event admin failed login summary	event
event-System-Summary-By-Severity	Event system summary by severity	event
event-System-Summary-By-Date	Event system summary by date	event
event-System-Critical-Severity-Events	Event system critical severity events	event
event-System-High-Severity-Events	Event system high severity events	event
event-System-Medium-Severity-Events	Event system medium severity events	event

ID/Name	Description	Log Type
utm-drilldown-Top-Users-By-Bandwidth	UTM drilldown top users by bandwidth usage	traffic
utm-drilldown-Traffic-Summary	UTM drilldown traffic summary	traffic
utm-drilldown-Top-User-Destination	UTM drilldown top user destination	traffic
utm-drilldown-Email-Senders-Summary	UTM drilldown email senders summary	traffic
utm-drilldown-Email-Receivers-Summary	UTM drilldown email receivers summary	traffic
utm-drilldown-Top-Email-Recipients	UTM drilldown top email recipients	traffic
utm-drilldown-Top-Email-Senders	UTM drilldown top email senders	traffic
utm-drilldown-Top-Allowed-Web-Sites-By-Request	UTM drilldown top allowed web sites by request	traffic
utm-drilldown-Top-Blocked-Web-Sites-By-Request	UTM drilldown top blocked web sites by request	traffic
utm-drilldown-Top-Virus	UTM drilldown top virus	traffic
utm-drilldown-Top-Attacks-By-Name	UTM drilldown top attacks by name	attack
utm-drilldown-Top-Vulnerability-By-Name	UTM drilldown top vulnerability by name	netscan
utm-drilldown-Top-App-By-Bandwidth	UTM drilldown top applications by bandwidth usage	traffic
utm-drilldown-Top-App-By-Sessions	UTM drilldown top applications by session count	traffic
traffic-Top-Users-By-Bandwidth	Traffic top users by bandwidth usage	traffic
reputation-Score-Summary-For-All-Users-Devices	Reputation score summary for all users devices	traffic
reputation-Number-Of-Incidents-For-All-Users-Devices	Reputation number of incidents for all users devices	traffic
reputation-Top-Users-By-Scores	Reputation top users by scores	traffic
reputation-Top-Devices-By-Scores	Reputation top devices by scores	traffic
reputation-Top-Users-With-Increased-Scores	Reputation top users with increased scores	traffic

ID/Name	Description	Log Type
reputation-Top-Devices-With-Increased-Scores	Reputation top devices with increased scores	traffic
threat-Attacks-By-Severity	Threat attacks by severity	attack
threat-Top-Attacks-Detected	Threat top attacks detected	attack
threat-Top-Attacks-Blocked	Threat top attacks blocked	attack
threat-Intrusion-Timeline	Threat intrusion timeline	attack
threat-Top-Virus-Source	Threat top virus source	traffic
threat-Virus-Timeline	Threat virus timeline	virus
threat-Top-Spyware-Victims	Threat top spyware victims	virus
threat-Top-Spyware-by-Name	Threat top spyware by name	virus
threat-Top-Spyware-Source	Threat top spyware source	traffic
threat-Spyware-Timeline	Threat spyware timeline	virus
threat-Top-Adware-Victims	Threat top adware victims	virus
threat-Top-Adware-by-Name	Threat top adware by name	virus
threat-Top-Adware-Source	Threat top adware source	traffic
threat-Adware-Timeline	Threat adware timeline	virus
threat-Intrusions-Timeline-By-Severity	Threat intrusions timeline by severity	attack
threat-Top-Intrusions-By-Types	Threat top intrusions by types	attack
threat-Critical-Severity-Intrusions	Threat critical severity intrusions	attack
threat-High-Severity-Intrusions	Threat high severity intrusions	attack
threat-Medium-Severity-Intrusions	Threat medium severity intrusions	attack
threat-Low-Severity-Intrusions	Threat low severity intrusions	attack
threat-Top-Intrusion-Victims	Threat top intrusion victims	attack
threat-Top-Intrusion-Sources	Threat top intrusion sources	attack
threat-Top-Monitored-Intrusions	Threat top monitored intrusions	attack

ID/Name	Description	Log Type
threat-Top-Blocked-Intrusions	Threat top blocked intrusions	attack
threat-Attacks-Over-HTTP-HTTPs	Threat attacks over HTTP HTTPs	attack
default-AP-Detection-Summary-by-Status-OffWire	Default access point detection summary by status off-wire	event
default-AP-Detection-Summary-by-Status-OnWire	Default access point detection summary by status on-wire	event
default-Managed-AP-Summary	Default managed access point summary	event
default-Unclassified-AP-Summary	Default unclassified access point summary	event
default-selected-AP-Details-OnWire	Default selected access point details on-wire	event
default-selected-AP-Details-OffWire	Default selected access point details off-wire	event
event-Wireless-Client-Details	Event wireless client details	event
event-Wireless-Accepted-Offwire	Event wireless accepted off-wire	event
event-Wireless-Accepted-Onwire	Event wireless accepted on-wire	event
event-Wireless-Rogue-Offwire	Event wireless rogue off-wire	event
event-Wireless-Rogue-Onwire	Event wireless rogue on-wire	event
event-Wireless-Suppressed-Offwire	Event wireless suppressed off-wire	event
event-Wireless-Suppressed-Onwire	Event wireless suppressed on-wire	event
event-Wireless-Unclassified-Offwire	Event wireless unclassified off-wire	event
event-Wireless-Unclassified-Onwire	Event wireless unclassified on-wire	event
default-Top-IPSEC-Vpn-Dial-Up-User-By-Bandwidth	Default top IPsec VPN dial up user by bandwidth usage	event
default-Top-Dial-Up-User-Of-Vpn-Tunnel-By-Bandwidth	Default top dial up user of VPN tunnel by bandwidth usage	traffic
default-Top-Sources-Of-SSL-VPN-Tunnels-By-Bandwidth	Default top sources of SSL VPN tunnels by bandwidth usage	event

ID/Name	Description	Log Type
webfilter-Web-Activity-Summary-By-Requests	Webfilter web activity summary by requests	webfilter
traffic-Browsing-Time-Summary	Traffic browsing time summary	traffic
webfilter-Top-Web-Users-By-Blocked-Requests	Webfilter top web users by blocked requests	webfilter
webfilter-Top-Web-Users-By-Allowed-Requests	Webfilter top web users by allowed requests	webfilter
webfilter-Top-Web-Users-By-Bandwidth	Webfilter top web users by bandwidth usage	webfilter
webfilter-Top-Blocked-Web-Sites-By-Requests	Webfilter top blocked web sites by requests	webfilter
webfilter-Top-Allowed-Web-Sites-By-Requests	Webfilter top allowed web sites by requests	webfilter
webfilter-Top-Allowed-Web-Sites-by-Bandwidth	Webfilter top allowed web sites by bandwidth usage	webfilter
webfilter-Top-Video-Streaming-Websites-By-Bandwidth	Webfilter top video streaming websites by bandwidth usage	webfilter
webfilter-Top-Blocked-Web-Categories	Webfilter top blocked web categories	webfilter
webfilter-Top-Allowed-Web-Categories	Webfilter top allowed web categories	webfilter
traffic-Top-Web-Users-By-Browsing-Time	Traffic top web users by browsing time	traffic
traffic-Top-Domains-By-Browsing-Time	Traffic top domains by browsing time	traffic
traffic-Top-Sites-By-Browsing-Time	Traffic top sites by browsing time	traffic
traffic-Top-Category-By-Browsing-Time	Traffic top category by browsing time	traffic
webfilter-Categories-By-Bandwidth	Webfilter categories by bandwidth usage	webfilter
traffic-Top-Destination-Countries-By-Browsing-Time	Traffic top destination countries by browsing time	traffic
webfilter-Top-Search-Phrases	Webfilter top search phrases	webfilter
Estimated-Browsing-Time	Estimated browsing time	traffic
wifi-Top-AP-By-Bandwidth	Top access point by bandwidth usage	traffic

ID/Name	Description	Log Type
wifi-Top-AP-By-Client	Top access point by client	traffic
wifi-Top-SSID-By-Bandwidth	Top SSIDs by bandwidth usage	traffic
wifi-Top-SSID-By-Client	Top SSIDs by client	traffic
wifi-Top-App-By-Bandwidth	Top WiFi applications by bandwidth usage	traffic
wifi-Top-Client-By-Bandwidth	Top WiFi client by bandwidth usage	traffic
wifi-Top-OS-By-Bandwidth	Top WiFi os by bandwidth usage	traffic
wifi-Top-OS-By-WiFi-Client	Top WiFi os by WiFi client	traffic
wifi-Top-Device-By-Bandwidth	Top WiFi device by bandwidth usage	traffic
wifi-Top-Device-By-Client	Top WiFi device by client	traffic
wifi-Overall-Traffic	WiFi overall traffic	traffic
wifi-Num-Distinct-Client	WiFi num distinct client	traffic
app-Top-Category-and-Applications-by-Bandwidth	Top category and applications by bandwidth usage	traffic
app-Top-Category-and-Applications-by-Session	Top category and applications by session	traffic
app-Top-Allowed-Applications-by-Bandwidth	Top allowed applications by bandwidth usage	traffic
app-Top-Blocked-Applications-by-Session	Top blocked applications by session	traffic
traffic-User-Detail	Traffic user details	traffic
web-Detailed-Website-Browsing-Log	Web detailed website browsing log	traffic
web-Hourly-Category-and-Website-Hits-Action	Web hourly category and website hits action	traffic
web-Top-Category-and-Websites-by-Bandwidth	Web top category and websites by bandwidth usage	traffic
web-Top-Category-and-Websites-by-Session	Web top category and websites by session	traffic
web-Top-Website-Sessions-by-Bandwidth	Web top website sessions by bandwidth usage	traffic

ID/Name	Description	Log Type
web-Top-User-Visted-Websites-by-Band-width	Web top user visted websites by bandwidth usage	traffic
web-Top-User-Visted-Websites-by-Session	Web top user visted websites by session	traffic
os-Detect-OS-Count	Detected operation system count	traffic
drilldown-Top-App-By-Sessions	Drilldown top applications by session count	traffic
drilldown-Top-App-By-Bandwidth	Drilldown top applications by bandwidth usage	traffic
drilldown-Top-Destination-By-Sessions	Drilldown top destination by session count	traffic
drilldown-Top-Destination-By-Bandwidth	Drilldown top destination by bandwidth usage	traffic
drilldown-Top-User-By-Sessions	Drilldown top user by session count	traffic
drilldown-Top-User-By-Bandwidth	Drilldown top user by bandwidth usage	traffic
drilldown-Top-Web-User-By-Visit	Drilldown top web user by visit	traffic
drilldown-Top-Website-By-Request	Drilldown top website by request	traffic
drilldown-Top-Email-Sender-By-Volume	Drilldown top email sender by volume	traffic
drilldown-Top-Email-Sender-By-Count	Drilldown top email sender by count	traffic
drilldown-Top-Email-Send-Recipient-By-Volume	Drilldown top email send recipient by volume	traffic
drilldown-Top-Email-Send-Recipient-By-Count	Drilldown top email send recipient by count	traffic
drilldown-Top-Email-Receiver-By-Volume	Drilldown top email receiver by volume	traffic
drilldown-Top-Email-Receiver-By-Count	Drilldown top email receiver by count	traffic
drilldown-Top-Email-Receive-Sender-By-Volume	Drilldown top email receive sender by volume	traffic
drilldown-Top-Email-Receive-Sender-By-Count	Drilldown top email receive sender by count	traffic
drilldown-Top-Attack-Dest	Drilldown top attack dest	attack
drilldown-Top-Attack-Source	Drilldown top attack source	attack

ID/Name	Description	Log Type
drilldown-Top-Attack-List	Drilldown top attack list	attack
drilldown-Virus-Detail	Drilldown virus detail	traffic
user-drilldown-Top-Blocked-Web-Sites-By-Requests	User drilldown top blocked web sites by requests	webfilter
user-drilldown-Top-Allowed-Web-Sites-By-Requests	User drilldown top allowed web sites by requests	webfilter
user-drilldown-Top-Blocked-Web-Categories	User drilldown top blocked web categories	webfilter
user-drilldown-Top-Allowed-Web-Categories	User drilldown top allowed web categories	webfilter
user-drilldown-Top-Attacks-By-Name	User drilldown top attacks by name	attack
user-drilldown-Top-Attacks-High-Severity	User drilldown top attacks high severity	attack
user-drilldown-Top-Virus	User drilldown top virus	virus
user-drilldown-Top-Virus-Receivers-Over-Email	User drilldown top virus receivers over email	virus
user-drilldown-Count-Spam-Activity-by-Hour-of-Day	User drilldown count spam activity by hour of day	emailfilter
user-drilldown-Top-Spam-Sources	User drilldown top spam sources	emailfilter
event-Usage-CPU	Event usage CPU	event
event-Usage-Mem	Event usage memory	event
event-Usage-Sessions	Event usage sessions	event
event-Usage-CPU-Sessions	Event usage CPU sessions	event
bandwidth-app-Top-Users-By-Bandwidth	Bandwidth application top users by bandwidth usage	traffic
bandwidth-app-Traffic-By-Active-User-Number	Bandwidth application traffic by active user number	traffic
bandwidth-app-Top-Dest-By-Bandwidth-Sessions	Bandwidth application top dest by bandwidth usage sessions	traffic
bandwidth-app-Traffic-Statistics	Bandwidth application traffic statistics	traffic

ID/Name	Description	Log Type
App-Risk-Top-User-Source-By-Sessions	Application risk top user source by session count	traffic
App-Risk-Reputation-Top-Users-By-Scores	Application risk reputation top users by scores	traffic
App-Risk-Reputation-Top-Devices-By-Scores	Application risk reputation top devices by scores	traffic
App-Risk-App-Usage-By-Category	Application risk application usage by category	traffic
App-Risk-Application-Activity-APP	Application risk application activity	traffic
App-Risk-Applications-Running-Over-HTTP	Application risk applications running over HTTP	traffic
App-Risk-Web-Browsing-Summary-Category	Application risk web browsing summary category	traffic
App-Risk-Web-Browsing-Activity-Hostname-Category	Application risk web browsing activity hostname category	traffic
App-Risk-Top-Threat-Vectors	Application risk top threat vectors	attack
App-Risk-Top-Critical-Threat-Vectors	Application risk top critical threat vectors	attack
App-Risk-Top-High-Threat-Vectors	Application risk top high threat vectors	attack
App-Risk-Top-Medium-Threat-Vectors	Application risk top medium threat vectors	attack
App-Risk-Top-Low-Threat-Vectors	Application risk top low threat vectors	attack
App-Risk-Top-Info-Threat-Vectors	Application risk top info threat vectors	attack
App-Risk-DLP-UTM-Event	Application risk DLP UTM event	traffic
App-Risk-Vulnerability-Discovered	Application risk vulnerability discovered	netscan
App-Risk-Virus-Discovered	Application risk virus discovered	traffic
App-Risk-Breakdown-Of-Risk-Applications	Application risk breakdown of risk applications	traffic
App-Risk-Number-Of-Applications-By-Risk-Behavior	Application risk number of applications by risk behavior	traffic
App-Risk-High-Risk-Application	Application risk high risk application	traffic

ID/Name	Description	Log Type
appctrl-Top-Blocked-SCCP-Callers	Appctrl top blocked SCCP callers	app-ctrl
appctrl-Top-Blocked-SIP-Callers	Appctrl top blocked SIP callers	app-ctrl
content-Count-Total-SCCP-Call-Registrations-by-Hour-of-Day	Content count total SCCP call registrations by hour of day	content
content-Count-Total-SCCP-Calls-Duration-by-Hour-of-Day	Content count total SCCP calls duration by hour of day	content
content-Count-Total-SCCP-Calls-per-Status	Content count total SCCP calls per status	content
content-Count-Total-SIP-Call-Registrations-by-Hour-of-Day	Content count total SIP call registrations by hour of day	content
content-Count-Total-SIP-Calls-per-Status	Content count total SIP calls per status	content
content-Dist-Total-SIP-Calls-by-Duration	Content dist total SIP calls by duration	content
Botnet-Activity-By-Sources	Botnet activity by sources	traffic
Botnet-Infected-Hosts	Botnet infected hosts	traffic
Detected-Botnet	Detected botnet	traffic
Botnet-Sources	Botnet sources	traffic
Botnet-Victims	Botnet victims	traffic
Botnet-Timeline	Botnet timeline	traffic
Detailed-Application-Usage	Detailed application usage	traffic
Application-Session-History	Application session history	traffic
App-Sessions-By-Category	Application sessions by category	traffic
Top-P2P-App-By-Sessions	Top P2P applications by session count	traffic
Top-P2P-App-By-Bandwidth	Top P2P applications by bandwidth usage	traffic
High-Risk-Application-By-Bandwidth	High risk application by bandwidth usage	traffic
High-Risk-Application-By-Sessions	High risk application by session count	traffic
Top-Web-Sites-by-Bandwidth	Top web sites by bandwidth usage	webfilter

ID/Name	Description	Log Type
Top-Web-Sites-by-Sessions	Top web sites by session count	webfilter
Top-Web-Category-by-Bandwidth	Top web category by bandwidth usage	webfilter
Top-Web-Category-by-Sessions	Top web category by session count	webfilter
Total-Attack-Source	Total attack source	attack
Total-Number-of-Viruses	Total number of viruses	traffic
Total-Number-of-Botnet-Events	Total number of botnet events	traffic

Predefined macros

The following table lists the predefined macros for FortiGate.

Name	Description	Category
App Category with Highest Session Count	App Category with Highest Session Count	Traffic
Application with Highest Bandwidth	Application with Highest Bandwidth	Traffic
Application with Highest Session Count	Application with Highest Session Count	Traffic
Attack with Highest Session Count	Attack with Highest Session Count	Attack
Botnet with Highest Session Count	Botnet with Highest Session Count	Traffic
Destination with Highest Bandwidth	Destination with Highest Bandwidth	Traffic
Destination with Highest Session Count	Destination with Highest Session Count	Traffic
Highest Bandwidth Consumed (App Category)	Highest Bandwidth Consumed (App Category)	Traffic
Highest Bandwidth Consumed (Application)	Highest Bandwidth Consumed (Application)	Traffic
Highest Bandwidth Consumed (Destination)	Highest Bandwidth Consumed (Destination)	Traffic
Highest Bandwidth Consumed (P2P Application)	Highest Bandwidth Consumed (P2P Application)	Traffic
Highest Bandwidth Consumed (Source)	Highest Bandwidth Consumed (Source)	Traffic
Highest Bandwidth Consumed (Web Category)	Highest Bandwidth Consumed (Web Category)	Web Filter

Name	Description	Category
Highest Bandwidth Consumed (Website)	Highest Bandwidth Consumed (Website)	Web Filter
Highest Risk Application with Highest Bandwidth	Highest Risk Application with Highest Bandwidth	Traffic
Highest Risk Application with Highest Session Count	Highest Risk Application with Highest Session Count	Traffic
Highest Session Count (App Category)	Highest Session Count (App Category)	Traffic
Highest Session Count (Application)	Highest Session Count (Application)	Traffic
Highest Session Count (Attack)	Highest Session Count (Attack)	Attack
Highest Session Count (Botnet)	Highest Session Count (Botnet)	Traffic
Highest Session Count (Destination)	Highest Session Count (Destination)	Traffic
Highest Session Count (Highest Severity Attack)	Highest Session Count (Highest Severity Attack)	Attack
Highest Session Count (P2P Application)	Highest Session Count (P2P Application)	Traffic
Highest Session Count (Source)	Highest Session Count (Source)	Traffic
Highest Session Count (Virus)	Highest Session Count (Virus)	Traffic
Highest Session Count (Web Category)	Highest Session Count (Web Category)	Web Filter
Highest Session Count (Website)	Highest Session Count (Website)	Web Filter
Highest Severity Attack with Highest Session Count	Highest Severity Attack with Highest Session Count	Attack
P2P Application with Highest Bandwidth	P2P Application with Highest Bandwidth	Traffic
P2P Application with Highest Session Count	P2P Application with Highest Session Count	Traffic
Source with Highest Bandwidth	Source with Highest Bandwidth	Traffic
Source with Highest Session Count	Source with Highest Session Count	Traffic
Total Number of Attacks	Total Number of Attacks	Attack
Total Number of Botnet Events	Total Number of Botnet Events	Traffic
Total Number of Viruses	Total Number of Viruses	Traffic

Name	Description	Category
Virus with Highest Session Count	Virus with Highest Session Count	Traffic
Web Category with Highest Bandwidth	Web Category with Highest Bandwidth	Web Filter
Web Category with Highest Session Count	Web Category with Highest Session Count	Web Filter
Website with Highest Bandwidth	Website with Highest Bandwidth	Web Filter
Website with Highest Session Count	Website with Highest Session Count	Web Filter

FortiMail

Predefined charts

The following table lists the predefined charts for FortiMail.

Display Name	Description	Category
Average Size of Mails	Average size of mails in FortiMail history	FortiMail
History Average Size by Hour	Average size of messages per hour in FortiMail history	FortiMail
History Connections per Hour	Number of connections per hour in FortiMail history	FortiMail
History Messages per Hour	Number of mails per hour in FortiMail history	FortiMail
History Total Size by Hour	Total size of exchanged mails per hour in FortiMail history	FortiMail
Number of Mail Connections	Number of mail connections in FortiMail history	FortiMail
Number of Mails	Number of mails in FortiMail history	FortiMail
Top 20 Access List	Top 20 access list in FortiMail history	FortiMail
Top 20 IP Policy	Top 20 IP policy in FortiMail history	FortiMail
Top 20 Recipient Policy	Top 20 recipient policy in FortiMail history	FortiMail
Top 20 Subjects	Top 20 subjects in FortiMail history	FortiMail
Top Classifiers by Hour	Top classifiers by hour in FortiMail history	FortiMail

Display Name	Description	Category
Top Disposition Classifiers	Top disposition classifiers in FortiMail history	FortiMail
Top History Client Endpoint	Top 10 clients endpoint in FortiMail history	FortiMail
Top History Client IP	Top 10 client IP in FortiMail history	FortiMail
Top History Client MSISDN	Top 10 clients MSISDN in FortiMail history	FortiMail
Top History Local Recipient	Top 10 local recipients in FortiMail history	FortiMail
Top History Local Sender	Top 10 local senders in FortiMail history	FortiMail
Top History Local User	Top 10 local users in FortiMail history	FortiMail
Top History Local Virus Recipient	Top 10 local virus recipients in FortiMail history	FortiMail
Top History Local Virus Sender	Top 10 local virus senders in FortiMail history	FortiMail
Top History Mail Dest IP	Top 10 mail destination IP in FortiMail history	FortiMail
Top History Recipient	Top 10 recipients in FortiMail history	FortiMail
Top History Remote Address	Top 10 remote address in FortiMail history	FortiMail
Top History Remote Recipient	Top 10 remote recipients in FortiMail history	FortiMail
Top History Remote Sender	Top 10 remote senders in FortiMail history	FortiMail
Top History Remote Virus Recipient	Top 10 remote virus recipients in FortiMail history	FortiMail
Top History Remote Virus Sender	Top 10 remote virus senders in FortiMail history	FortiMail
Top History Sender	Top 10 senders in FortiMail history	FortiMail
Top History Sender Endpoint	Top 10 senders Endpoint in FortiMail history	FortiMail
Top History Sender IP	Top 10 sender IP in FortiMail history	FortiMail
Top History Sender MSISDN	Top 10 senders MSISDN in FortiMail history	FortiMail
Top History Total Active EmailAddress	Top 10 total active email address per domain	FortiMail
Top History Total Sent Received	Top 10 total sent received in FortiMail history	FortiMail

Display Name	Description	Category
Top History Virus	Top 10 viruses in FortiMail history	FortiMail
Top History Virus Dest IP	Top 10 virus destination IP in FortiMail history	FortiMail
Top History Virus Endpoint	Top 10 viruses endpoint in FortiMail history	FortiMail
Top History Virus IP	Top 10 virus IP in FortiMail history	FortiMail
Top History Virus MSISDN	Top 10 viruses MSISDN in FortiMail history	FortiMail
Top History Virus Recipient	Top 10 virus recipients in FortiMail history	FortiMail
Top History Virus Sender	Top 10 virus senders in FortiMail history	FortiMail
Top Spammed Domains	Top spammed domains in FortiMail history	FortiMail
Top Spammed Users	Top spammed users in FortiMail history	FortiMail
Total Message Delay	Total message delay in FortiMail history	FortiMail
Total Message TransmissionDelay	Total message transmissionDelay in FortiMail history	FortiMail
Total Size of Mails	Total size of mails in FortiMail history	FortiMail

Predefined datasets

The following table lists the predefined datasets for FortiMail.

ID/Name	Description	Log Type
fml-History-Top-Client-IP	FortiMail history top client IP	history
fml-History-Top-Local-User	FortiMail history top local user	history
fml-History-Top-Remote-Address	FortiMail history top remote address	history
fml-History-Top-Virus	FortiMail history top virus	history
fml-History-Top-Client-MSISDN	FortiMail history top client msisdn	history
fml-History-Top-Client-Endpoint	FortiMail history top client endpoint	history
fml-History-Top-Sender	FortiMail history top sender	history
fml-History-Top-Sender-IP	FortiMail history top sender IP	history

ID/Name	Description	Log Type
fml-History-Top-Local-Sender	FortiMail history top local sender	history
fml-History-Top-Remote-Sender	FortiMail history top remote sender	history
fml-History-Top-Sender-MSISDN	FortiMail history top sender msisdn	history
fml-History-Top-Sender-Endpoint	FortiMail history top sender endpoint	history
fml-History-Top-Recipient	FortiMail history top recipient	history
fml-History-Top-Local-Recipient	FortiMail history top local recipient	history
fml-History-Top-Remote-Recipient	FortiMail history top remote recipient	history
fml-History-Top-Mail-Dest-IP	FortiMail history top mail dest IP	history
fml-History-Count-Total-Sent-Received	FortiMail history count total sent received	history
fml-History-Top-Virus-Sender	FortiMail history top virus sender	history
fml-History-Top-Virus-IP	FortiMail history top virus IP	history
fml-History-Top-Local-Virus-Sender	FortiMail history top local virus sender	history
fml-History-Top-Remote-Virus-Sender	FortiMail history top remote virus sender	history
fml-History-Top-Virus-MSISDN	FortiMail history top virus msisdn	history
fml-History-Top-Virus-Endpoint	FortiMail history top virus endpoint	history
fml-History-Top-Virus-Recipient	FortiMail history top virus recipient	history
fml-History-Top-Local-Virus-Recipient	FortiMail history top local virus recipient	history
fml-History-Top-Remote-Virus-Recipient	FortiMail history top remote virus recipient	history
fml-History-Top-Virus-Dest-IP	FortiMail history top virus dest IP	history
fml-Active-EmailAddress-Summary	FortiMail active emailaddress summary	history
fml-Average-Size-by-Hour	FortiMail average size by hour	history
fml-Messages-per-Hour	FortiMail messages per hour	history
fml-Total-Size-by-Hour	FortiMail total size by hour	history
fml-Connections-per-Hour	FortiMail connections per hour	history

ID/Name	Description	Log Type
fml-history-Average-Size-of-Mails	FortiMail history average size of mails	history
fml-history-Total-Size-of-Mails	FortiMail history total size of mails	history
fml-history-Number-of-Mail-Connections	FortiMail history number of mail connections	history
fml-history-Number-of-Mails	FortiMail history number of mails	history
fml-history-Total-Message-Delay	FortiMail history total message delay	event
fml-history-Total-Message-Transmission-Delay	FortiMail history total message transmission delay	event
fml-history-Top-IP-Policy	FortiMail history top IP policy	history
fml-history-Top-Recipient-Policy	FortiMail history top recipient policy	history
fml-history-Top-Access-List	FortiMail history top access list	history
fml-history-Top-Spammed-Domains	FortiMail history top spammed domains	history
fml-history-Top-Spammed-Users	FortiMail history top spammed users	history
fml-history-Top-Classifiers-By-Hour	FortiMail history top classifiers by hour	history
fml-history-Top-Disposition-Classifiers	FortiMail history top disposition classifiers	history
fml-history-Top-Subjects	FortiMail history top subjects	history

FortiWeb

Predefined charts

The following table lists the predefined charts for FortiWeb.

Display Name	Description	Category
Top Attack Destinations by Source	Top 10 attacked destinations by source	FortiWeb
Top Attack Destinations by Type	Top 10 attacked destinations by type	FortiWeb
Top Attack Protocols by Type	Top 10 attack protocols by type	FortiWeb
Top Attack Severity by Action	Top 10 detected attack severities by action	FortiWeb

Display Name	Description	Category
Top Attack Sources	Top 10 sources of attacks	FortiWeb
Top Attack Types	Top 10 detected attack types	FortiWeb
Top Attack Types by Source	Top 10 detected attack types by source	FortiWeb
Top Attack URLs	Top 10 detected attack URLs	FortiWeb
Top Attacked Destinations	Top 10 attacked destinations	FortiWeb
Top Attacked HTTP Methods by Type	Top 10 attacked HTTP methods by attack type	FortiWeb
Top Attacked User Identifications	Top 10 Attacked User identifications	FortiWeb
Top Attacks by Policy	Top 10 attacks used by policies	FortiWeb
Top Event Categories	Top 10 event categories	FortiWeb
Top Event Categories by Status	Top 10 event categories by status	FortiWeb
Top Event Login by User	Top 10 login events by user	FortiWeb
Top Event Types	Top 10 event types	FortiWeb
Top Traffic Destinations	Top 10 destinations in FortiWeb traffic	FortiWeb
Top Traffic Policies	Top 10 policies in FortiWeb traffic	FortiWeb
Top Traffic Services	Top 10 services in FortiWeb traffic	FortiWeb
Top Traffic Sources	Top 10 sources in FortiWeb traffic	FortiWeb

Predefined datasets

The following table lists the predefined datasets for FortiWeb.

ID/Name	Description	Log Type
fwb-attack-Top-Attack-Sources	FortiWeb attack top attack sources	attack
fwb-attack-Top-Attack-Types	FortiWeb attack top attack types	attack
fwb-attack-Top-Attack-URLs	FortiWeb attack top attack URLs	attack
fwb-attack-Top-Attack-Severities-By-Action	FortiWeb attack top attack severities by action	attack

ID/Name	Description	Log Type
fwb-attack-Top-Attack-Destinations-By-Type	FortiWeb attack top attack destinations by type	attack
fwb-attack-Top-Attack-Destinations-By-Source	FortiWeb attack top attack destinations by source	attack
fwb-attack-Top-Attack-Types-By-Source	FortiWeb attack top attack types by source	attack
fwb-attack-Top-Attacked-Http-Methods-By-Type	FortiWeb attack top attacked HTTP methods by type	attack
fwb-attack-Top-Attacks-By-Policy	FortiWeb attack top attacks by policy	attack
fwb-attack-Top-Attacked-Destinations	FortiWeb attack top attacked destinations	attack
fwb-attack-Top-Attack-Protocols-By-Type	FortiWeb attack top attack protocols by type	attack
fwb-attack-Top-Attacked-User-Identifications	FortiWeb attack top attacked user identifications	attack
fwb-traffic-Top-Policies	FortiWeb traffic top policies	traffic
fwb-traffic-Top-Services	FortiWeb traffic top services	traffic
fwb-traffic-Top-Sources	FortiWeb traffic top sources	traffic
fwb-traffic-Top-Destinations	FortiWeb traffic top destinations	traffic
fwb-event-Top-event-categories	FortiWeb event top event categories	event
fwb-event-Top-event-types	FortiWeb event top event types	event
fwb-event-Top-Event-Categories-By-Status	FortiWeb event top event categories by status	event
fwb-event-Top-login-by-user	FortiWeb event top login by user	event

FortiCache

Predefined charts

The following table lists the predefined charts for FortiCache.

Display Name	Description	Category
Top 20 Websites by Bandwidth Savings	Top 20 websites by bandwidth savings	FortiCache
Top 20 Websites by Cache Rate	Top 20 websites by cache rate	FortiCache
Top 20 Websites by Response Time Improvement	Top 20 websites by response time improvement	FortiCache

Predefined datasets

The following table lists the predefined datasets for FortiCache.

ID/Name	Description	Log Type
fch-Top-Websites-by-Bandwidth-Savings	Fetch the top websites by bandwidth savings	traffic
fch-Top-Websites-by-Cache-Rate	Fetch the top websites by cache rate	traffic
fch-Top-Websites-by-Response-Time-Improvement	Fetch the top websites by response time improvement	traffic

Appendix C - Port Numbers

The following tables describe the port numbers that the FortiAnalyzer unit uses:

- ports for traffic originating from units (outbound ports)
- ports for traffic receivable by units (listening ports)
- ports used to connect to the FortiGuard Distribution Network (FDN).

Traffic varies by enabled options and configured ports. Only default ports are listed.

Functionality	Port(s)
DNS lookup	UDP 53
NTP synchronization	UDP 123
Windows share	UDP 137-138
SNMP traps	UDP 162
Syslog, log forwarding	UDP 514 If a secure connection has been configured between a FortiGate device and a FortiAnalyzer device, syslog traffic will be sent into an IPsec tunnel. Data will be exchanged over UDP 500/4500, Protocol IP/50.
Log and report upload	TCP 21 or TCP 22
SMTP alert email	TCP 25
User name LDAP queries for reports	TCP 389 or TCP 636
RADIUS authentication	TCP 1812
TACACS+ authentication	TCP 49
Log aggregation client	TCP 3000
Device registration of FortiGate or FortiManager units; remote access to quarantine, logs and reports from a FortiGate unit; remote management from a FortiManager unit (configuration retrieval) (OFTP)	TCP 514

Functionality	Port(s)
Syslog, log forwarding	UDP 514 If a secure connection has been configured between a FortiGate and a FortiAnalyzer, syslog traffic will be sent into an IPsec tunnel. Data will be exchanged over UDP 500/4500, Protocol IP/50.
SSH administrative access to the CLI	TCP 22
Telnet administrative access to the CLI	TCP 23
HTTP administrative access to the GUI	TCP 80
HTTPS administrative access to the GUI; remote management from a FortiManager unit	TCP 443
Device registration of FortiGate or FortiManager units; remote access to quarantine, logs and reports from a FortiGate unit; remote management from a FortiManager unit (configuration retrieval) (OFTP)	TCP 514
HTTP or HTTPS administrative access to the GUI's CLI dashboard widget. Protocol used will match the protocol used by the administrator when logging in to the GUI.	TCP 2032
Log aggregation server Log aggregation server support requires model FortiAnalyzer 800 series or greater.	TCP 3000
Web Service	TCP 8080
Ping	ICMP protocol

Appendix D - Maximum Values Matrix

Maximum values per FortiAnalyzer model.

Feature	FAZ-100C, FAZ-200D	FAZ-300D, FAZ-400C	FAZ-1000C, FAZ-1000D	FAZ-3000D, FAZ-4000B	FAZ-3500E, FAZ-3900E	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
Administrative Domains (ADOMS)	100, 150	175, 200, 300	2000	2000	4000	10000	10000	10000	10000	10000
Administrators	256	256	256	256	256	256	256	256	256	256
Administrator access profiles	256	256	256	256	256	256	256	256	256	256
SNMP community	256	256	256	256	256	256	256	256	256	256
SNMP managers per community	256	256	256	256	256	256	256	256	256	256
Email servers	256	256	256	256	256	256	256	256	256	256
Syslog servers	256	256	256	256	256	256	256	256	256	256
TACACS+ servers	256	256	256	256	256	256	256	256	256	256
Administrator RADIUS servers	256	256	256	256	256	256	256	256	256	256
Administrator LDAP servers	256	256	256	256	256	256	256	256	256	256
Static routes	256	256	256	256	256	256	256	256	256	256
Log devices	100, 150	175, 200, 300	2000	2000	256	10000	10000	10000	10000	10000
Devices per ADOM	100, 150	175, 200, 300	2000	2000	4000	10000	10000	10000	10000	10000

Feature	FAZ-100C, FAZ-200D	FAZ-300D, FAZ-400C	FAZ-1000C, FAZ-1000D	FAZ-3000D, FAZ-4000B	FAZ-3500E, FAZ-3900E	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
Device Group Management	100, 150	175, 200, 300	2000	2000	4000	10000	10000	10000	10000	10000
Report output profiles	250	250	500	1000	1000	1000	1000	1000	1000	1000
SQL report templates	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL report charts	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL report datasets	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL database size (GB)	1000	4000, 1000, 2000	1000, 8000	16K, 6K, 24K		200	+200	+1000	+8K	+16K

Appendix E - SNMP MIB Support

The FortiAnalyzer SNMP agent supports the following MIBs:

MIB or RFC	Description
FORTINET-CORE-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for FortiAnalyzer-specific information and to receive FortiAnalyzer-specific traps.
RFC-1213 (MIB II)	The FortiAnalyzer SNMP agent supports MIB II groups, except: • There is no support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, etc.) do not accurately capture all FortiAnalyzer traffic activity. More accurate information can be obtained from the information reported by the FortiAnalyzer MIB.
RFC-2665 (Ethernet-like MIB)	The FortiAnalyzer SNMP agent supports Ethernet-like MIB information except the dot3Tests and dot3Errors groups.

You can obtain these MIB files from the Customer Service & Support portal: https://support.fortinet.com.

To be able to communicate with your FortiAnalyzer unit's SNMP agent, you must first compile these MIBs into your SNMP manager. If the standard MIBs used by the SNMP agent are already compiled into your SNMP manager, you do not have to compile them again.

To view a trap or query's name, object identifier (OID), and description, open its MIB file in a plain text editor.

All traps that are sent include the message, the FortiAnalyzer unit's serial number, and the host name.

SNMP MIB Files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib* MIB file in the firmware image file folder. The *FORTINET-CORE-MIB.mib* file is located in the main FortiAnalyzer v5.00 file folder.

FORTINET-CORE-MIB

```
--
-- FORTINET-CORE-MIB.mib: Main MIB for Fortinet enterprise OID tree
--
-- MODULE-IDENTITY
```

```
--  OrgName
--     Fortinet Technologies, Inc.
--  ContactInfo
--     Technical Support
--     e-mail: support@fortinet.com
--     http://www.fortinet.com
--


FORTINET-CORE-MIB DEFINITIONS ::= BEGIN

IMPORTS
    ifIndex
        FROM IF-MIB
    InetAddress, InetAddressPrefixLength, InetAddressType
        FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    sysName
        FROM SNMPv2-MIB
    Integer32, MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE,
    enterprises
        FROM SNMPv2-SMI
    DisplayString, TEXTUAL-CONVENTION
        FROM SNMPv2-TC;

fortinet MODULE-IDENTITY
    LAST-UPDATED "201205090000Z"
    ORGANIZATION
        "Fortinet Technologies, Inc."
    CONTACT-INFO
        "Technical Support
         email: support@fortinet.com
         http://www.fortinet.com
        "
    DESCRIPTION
        "Added fan failure and AMC bypass traps"
    REVISION    "201205090000Z"
    DESCRIPTION
        "Registered FortiDDoSMib OID"
    REVISION    "201204230000Z"
    DESCRIPTION
        "Registered FortiDNSMib OID"
    REVISION    "201112230000Z"
    DESCRIPTION
        "Registered FortiCacheMib OID"
    REVISION    "201104250000Z"
    DESCRIPTION
        "Supporting portuguese language"
    REVISION    "201005140000Z"
    DESCRIPTION
        "Registered FortiScanMib OID"
```

```
    REVISION    "200905200000Z"
    DESCRIPTION
        "MIB module for Fortinet network devices."
    REVISION    "200811190000Z"
    DESCRIPTION
        "Registered FortiWebMib OID"
    REVISION    "200810210000Z"
    DESCRIPTION
        "Added SMI comments"
    REVISION    "200806250000Z"
    DESCRIPTION
        "Adjusted fnAdmin tree to start at .1"
    REVISION    "200806160000Z"
    DESCRIPTION
        "Spelling corrections."
    REVISION    "200804170000Z"
    DESCRIPTION
        "Initial version of fortinet core MIB."
    ::= { enterprises 12356 }  -- assigned by IANA


--
-- Fortinet MIB Textual Conventions (TC)
--

FnBoolState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Boolean data type representing enabled/disabled"
    SYNTAX      INTEGER {
        disabled (1),
        enabled (2)
    }

FnLanguage ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Enumerated type for user interface languages"
    SYNTAX      INTEGER {
        english (1),
        simplifiedChinese (2),
        japanese (3),
        korean (4),
        spanish (5),
        traditionalChinese (6),
        french (7),
        portuguese (8),
        undefined (255)
    }

FnIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
```

```
    STATUS      current
    DESCRIPTION
        "Data type for table index values"
    SYNTAX      Integer32 (0..2147483647)

FnSessionProto ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Data type for session protocols"
    SYNTAX      INTEGER {
        ip (0),
        icmp (1),
        igmp (2),
        ipip (4),
        tcp (6),
        egp (8),
        pup (12),
        udp (17),
        idp (22),
        ipv6 (41),
        rsvp (46),
        gre (47),
        esp (50),
        ah (51),
        ospf (89),
        pim (103),
        comp (108),
        raw (255)
    }

--
-- Fortinet Enterprise Structure of Management Information (SMI)
--

fnCoreMib OBJECT IDENTIFIER ::= { fortinet 100 }

--
-- Fortinet Product Family MIB Object Identifier Assignments
--
-- fnFortiGateMib     OBJECT IDENTIFIER ::= { fortinet 101 }
-- fnFortiAnalyzerMib OBJECT IDENTIFIER ::= { fortinet 102 }
-- fnFortiManagerMib  OBJECT IDENTIFIER ::= { fortinet 103 }
-- fnFortiDefenderMib OBJECT IDENTIFIER ::= { fortinet 104 }
-- fnFortiMailMib     OBJECT IDENTIFIER ::= { fortinet 105 }
-- fnFortiSwitchMib   OBJECT IDENTIFIER ::= { fortinet 106 }
-- fnFortiWebMib      OBJECT IDENTIFIER ::= { fortinet 107 }
-- fnFortiScanMib     OBJECT IDENTIFIER ::= { fortinet 108 }
-- fnFortiCacheMib    OBJECT IDENTIFIER ::= { fortinet 109 }
-- fnFortiDNSMib      OBJECT IDENTIFIER ::= { fortinet 110 }
-- fnFortiDDoSMib     OBJECT IDENTIFIER ::= { fortinet 111 }
--
```

```
--
-- fnCoreMib.fnCommon
--
fnCommon OBJECT IDENTIFIER ::= { fnCoreMib 1 }

--
-- fnCoreMib.fnCommon.fnSystem
--
fnSystem OBJECT IDENTIFIER ::= { fnCommon 1 }

fnSysSerial OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Device serial number. This is the same serial number as given
        in the ENTITY-MIB tables for the base entity."
    ::= { fnSystem 1 }

--
-- fnCoreMib.fnCommon.fnMgmt
--
fnMgmt OBJECT IDENTIFIER ::= { fnCommon 2 }

fnMgmtLanguage OBJECT-TYPE
    SYNTAX      FnLanguage
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Language used for administration interfaces"
    ::= { fnMgmt 1 }

fnAdmin OBJECT IDENTIFIER ::= { fnMgmt 100 }

fnAdminNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of admin accounts in fnAdminTable"
    ::= { fnAdmin 1 }

fnAdminTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FnAdminEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of administrator accounts on the device. This table is
        intended to be extended with platform specific information."
    ::= { fnAdmin 2 }

fnAdminEntry OBJECT-TYPE
```

```
    SYNTAX      FnAdminEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable to a particular admin account"
    INDEX       { fnAdminIndex }
    ::= { fnAdminTable 1 }

FnAdminEntry ::= SEQUENCE {
    fnAdminIndex        Integer32,
    fnAdminName         DisplayString,
    fnAdminAddrType     InetAddressType,
    fnAdminAddr         InetAddress,
    fnAdminMask         InetAddressPrefixLength
}

fnAdminIndex OBJECT-TYPE
    SYNTAX      Integer32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index uniquely defining an administrator account within the fnAd-
minTable"
    ::= { fnAdminEntry 1 }

fnAdminName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The user-name of the specified administrator account"
    ::= { fnAdminEntry 2 }

fnAdminAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The type of address stored in fnAdminAddr, in compliance with INET-
ADDRESS-MIB"
    ::= { fnAdminEntry 3 }

fnAdminAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The address prefix identifying where the administrator account can
        be used from, typically an IPv4 address. The address type/format is
        determined by fnAdminAddrType."
    ::= { fnAdminEntry 4 }
```

```
fnAdminMask OBJECT-TYPE
    SYNTAX      InetAddressPrefixLength
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The address prefix length (or network mask) applied to the fgAdminAddr
        to determine the subnet or host the administrator can access the device
from"
    ::= { fnAdminEntry 5 }

--
-- fnCoreMib.fnCommon.fnTraps
--
fnTraps OBJECT IDENTIFIER ::= { fnCommon 3 }

fnTrapsPrefix OBJECT IDENTIFIER ::= { fnTraps 0 }

fnTrapObjects OBJECT IDENTIFIER ::= { fnTraps 1 }

fnGenTrapMsg OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Generic message associated with an event. The content will
        depend on the nature of the trap."
    ::= { fnTrapObjects 1 }

fnTrapCpuThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates that the CPU usage has exceeded the configured threshold."
    ::= { fnTrapsPrefix 101 }

fnTrapMemThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates memory usage has exceeded the configured threshold."
    ::= { fnTrapsPrefix 102 }

fnTrapLogDiskThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Log disk usage has exceeded the configured threshold. Only available
        on devices with log disks."
    ::= { fnTrapsPrefix 103 }

fnTrapTempHigh NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
```

```
    STATUS      current
    DESCRIPTION
        "A temperature sensor on the device has exceeded its threshold.
        Not all devices have thermal sensors. See manual for specifications."
    ::= { fnTrapsPrefix 104 }

fnTrapVoltageOutOfRange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Power levels have fluctuated outside of normal levels. Not all devices
        have voltage monitoring instrumentation. See manual for specifications."
    ::= { fnTrapsPrefix 105 }

fnTrapPowerSupplyFailure NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Power supply failure detected. Not available on all models. Available
        on some devices which support redundant power supplies. See manual
        for specifications."
    ::= { fnTrapsPrefix 106 }

fnTrapAmcIfBypassMode NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "An AMC interface entered bypass mode. Available on models with an AMC
        expansion slot. Used with the ASM-CX4 and ASM-FX2 cards."
    ::= { fnTrapsPrefix 107 }

fnTrapFanFailure NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "A fan failure has been detected. Not all devices have fan sensors.
        See manual for specifications."
    ::= { fnTrapsPrefix 108 }

fnTrapIpChange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, ifIndex }
    STATUS      current
    DESCRIPTION
        "Indicates that the IP address of the specified interface has been
changed."
    ::= { fnTrapsPrefix 201 }

fnTrapTest NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Trap sent for diagnostic purposes by an administrator."
```

```
    ::= { fnTrapsPrefix 999 }

--
-- fnCoreMib.fnCommon.fnMIBConformance
--
fnMIBConformance OBJECT IDENTIFIER ::= { fnCoreMib 10 }

fnSystemComplianceGroup OBJECT-GROUP
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "Objects relating to the physical device."
    ::= { fnMIBConformance 1 }

fnMgmtComplianceGroup OBJECT-GROUP
    OBJECTS     { fnMgmtLanguage }
    STATUS      current
    DESCRIPTION
        "Objects relating the management of a device."
    ::= { fnMIBConformance 2 }

fnAdminComplianceGroup OBJECT-GROUP
    OBJECTS     { fnAdminNumber, fnAdminName, fnAdminAddrType,
                  fnAdminAddr, fnAdminMask }
    STATUS      current
    DESCRIPTION
        "Administration access control objects."
    ::= { fnMIBConformance 3 }

fnTrapsComplianceGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fnTrapCpuThreshold, fnTrapMemThreshold,
                    fnTrapLogDiskThreshold, fnTrapTempHigh,
                    fnTrapVoltageOutOfRange, fnTrapPowerSupplyFailure,
                    fnTrapAmcIfBypassMode, fnTrapFanFailure,
                    fnTrapIpChange, fnTrapTest }
    STATUS      current
    DESCRIPTION
        "Event notifications"
    ::= { fnMIBConformance 4 }

fnNotifObjectsComplianceGroup OBJECT-GROUP
    OBJECTS     { fnGenTrapMsg }
    STATUS      current
    DESCRIPTION
        "Object identifiers used in notifications"
    ::= { fnMIBConformance 5 }

fnMIBCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
        "The compliance statement for the application MIB."
```

```
    MODULE      -- this module

        GROUP   fnSystemComplianceGroup
        DESCRIPTION
              "This group is mandatory for all Fortinet network appliances
              supporting this MIB."

        GROUP   fnMgmtComplianceGroup
        DESCRIPTION
              "This group is optional for devices that do not support common
              management interface options such as multiple languages."

        GROUP   fnAdminComplianceGroup
        DESCRIPTION
              "This group should be accessible on any device supporting
              administrator authentication."

        GROUP   fnTrapsComplianceGroup
        DESCRIPTION
              "Traps are optional. Not all models support all traps. Consult
              product literature to see which traps are supported."

        GROUP   fnNotifObjectsComplianceGroup
        DESCRIPTION
              "Object identifiers used in notifications. Objects are required
              if their containing trap is implemented."

    ::= { fnMIBConformance 100 }

END
```

FORTINET-FORTIMANAGER-FORTIANALYZER-MIB

```
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB DEFINITIONS ::= BEGIN

IMPORTS
    fnSysSerial, fortinet, FnIndex, fnGenTrapMsg
        FROM FORTINET-CORE-MIB
    sysName
        FROM SNMPv2-MIB
    InetPortNumber
        FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE,
    Integer32, Gauge32, Counter32, IpAddress
        FROM SNMPv2-SMI
    DisplayString, TEXTUAL-CONVENTION
        FROM SNMPv2-TC;
```

```
fnFortiManagerMib MODULE-IDENTITY
    LAST-UPDATED "201404220000Z"
    ORGANIZATION
        "Fortinet Technologies, Inc."
    CONTACT-INFO
        "
         Technical Support
         email: support@fortinet.com
         http://www.fortinet.com"
    DESCRIPTION
         "Add model names faz3000E, fmg4000E, faz1000D, fmg1000D."
    REVISION    "201404220000Z"
    DESCRIPTION
         "Added fmSysCpuUsageExcludedNice.
          Added fmTrapCpuThresholdExcludeNice."
    REVISION    "201306100000Z"
    DESCRIPTION
         "Add support for FortiAnalyzer."
    REVISION    "201303270000Z"
    DESCRIPTION
         "Added license gb/day and device quota trap. fmTrapLicGbDayThreshold
          and fmTrapLicDevQuotaThreshold"
    REVISION    "201211260000Z"
    DESCRIPTION
         "Added commas between notifications in NOTIFICATION-GROUP.
          Added imports from SNMPv2-SMI and SNMPv2-TC.
          imported `OBJECT-GROUP' from module SNMPv2-CONF"
    REVISION    "201204200000Z"
    DESCRIPTION
         "Added RAID trap fmTrapRAIDStatusChange."
    REVISION    "201103250000Z"
    DESCRIPTION
        "Added fmSysMemUsed,fmSysMemCapacity,fmSysCpuUsage.
         Added new FortiManager models."
    REVISION    "201101190000Z"
    DESCRIPTION
        "MIB module for Fortinet FortiManager devices."
    REVISION    "200807180000Z"
    DESCRIPTION
        "Add sysName to fmTrapHASwitch."
    REVISION    "200806260000Z"
    DESCRIPTION
        "OID correction for fnFortiManagerMib."
    REVISION    "200806160000Z"
    DESCRIPTION
        "Spelling corrections."
    REVISION    "200806100000Z"
    DESCRIPTION
        "Initial version of FORTINET-FORTIMANAGER-MIB."
    ::= { fortinet 103 }
```

```
--
-- fortinet.fnFortiManagerMib.fmTraps
--

FmRAIDStatusCode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Enumerated list of RAID status codes."
    SYNTAX      INTEGER { arrayOK(1), arrayDegraded(2), arrayFailed(3),
                   arrayRebuilding(4), arrayRebuildingStarted(5),
                   arrayRebuildingFinished(6), arrayInitializing(7),
                    arrayInitializingStarted(8), arrayInitializingFinished(9),
                    diskOK(10), diskDegraded(11), diskFailEvent(12) }

FmSessProto ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "data type for session protocols"
    SYNTAX      INTEGER { ip(0), icmp(1), igmp(2), ipip(4), tcp(6),
                          egp(8), pup(12), udp(17), idp(22), ipv6(41),
                          rsvp(46), gre(47), esp(50), ah(51), ospf(89),
                          pim(103), comp(108), raw(255) }


fmTraps OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 0 }

fmTrapPrefix OBJECT IDENTIFIER
    ::= { fmTraps 0 }

fmTrapObject OBJECT IDENTIFIER
    ::= { fmTraps 1 }

fmRAIDStatus OBJECT-TYPE
    SYNTAX      FmRAIDStatusCode
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "New RAID state associated with a RAID status change event."
    ::= { fmTrapObject 1 }

fmRAIDDevIndex OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Name/index of a RAID device relating to the event."
    ::= { fmTrapObject 2 }

fmLogRate OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
```

```
    STATUS      current
    DESCRIPTION
        "Log receiving rate in number of logs per second."
    ::= { fmTrapObject 3 }

fmLogRateThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Threshold for log rate in number of logs per second."
    ::= { fmTrapObject 4 }

fmLogDataRate OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log receiving data rate in number of KB per second."
    ::= { fmTrapObject 5 }

fmLogDataRateThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Threshold for log data rate in number of KB per second."
    ::= { fmTrapObject 6 }

fmLicGbDay OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log data used in number of GB per day."
    ::= { fmTrapObject 7 }

fmLicGbDayThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Licensed threshold for log data in number of GB per day."
    ::= { fmTrapObject 8 }

fmLicDevQuota OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Device quota used in number of GB."
    ::= { fmTrapObject 9 }
```

```
fmLicDevQuotaThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Licensed threshold for device quota in number of GB."
    ::= { fmTrapObject 10 }

--
-- fortinet.fnFortiManagerMib.fmModel
--

fmModel OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 1 }

fmg100 OBJECT IDENTIFIER
    ::= { fmModel 1000 }

fmgvm OBJECT IDENTIFIER
    ::= { fmModel 1001 }

fmg100C OBJECT IDENTIFIER
    ::= { fmModel 1003 }

fmg200D OBJECT IDENTIFIER
    ::= { fmModel 2004 }

fmg300D OBJECT IDENTIFIER
    ::= { fmModel 3004 }

fmg400 OBJECT IDENTIFIER
    ::= { fmModel 4000 }

fmg400A OBJECT IDENTIFIER
    ::= { fmModel 4001 }

fmg400B OBJECT IDENTIFIER
    ::= { fmModel 4002 }

fmg400C OBJECT IDENTIFIER
    ::= { fmModel 4003 }

fmg1000C OBJECT IDENTIFIER
    ::= { fmModel 10003 }

fmg1000D OBJECT IDENTIFIER
    ::= { fmModel 10004 }

fmg2000XL OBJECT IDENTIFIER
    ::= { fmModel 20000 }
```

```
fmg3000 OBJECT IDENTIFIER
    ::= { fmModel 30000 }

fmg3000B OBJECT IDENTIFIER
    ::= { fmModel 30002 }

fmg3000C OBJECT IDENTIFIER
    ::= { fmModel 30003 }

fmg4000D OBJECT IDENTIFIER
    ::= { fmModel 40004 }

fmg4000E OBJECT IDENTIFIER
    ::= { fmModel 40005 }

fmg5001A OBJECT IDENTIFIER
    ::= { fmModel 50011 }

--
-- fortinet.fnFortiManagerMib.fmSystem
--

fmSystem OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 2 }

--
-- fortinet.fnFortiManagerMib.fmSystem.fmSystemInfo
--

fmSystemInfo OBJECT IDENTIFIER
    ::= { fmSystem 1 }

fmSysCpuUsage OBJECT-TYPE
    SYNTAX      Integer32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current CPU usage (percentage)"
    ::= { fmSystemInfo 1 }

fmSysMemUsed OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory used (KB)"
    ::= { fmSystemInfo 2 }

fmSysMemCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Total physical and swap memory installed (KB)"
    ::= { fmSystemInfo 3 }

fmSysDiskUsage OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current hard disk usage (MB)"
    ::= { fmSystemInfo 4 }

fmSysDiskCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total hard disk capacity (MB)"
    ::= { fmSystemInfo 5 }

fmSysCpuUsageExcludedNice OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current CPU usage excluded nice processes usage (percentage)"
    ::= { fmSystemInfo 6 }

fmTrapHASwitch NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "FortiManager HA cluster has been re-arranged. A new master has been selec-
ted and asserted."
    ::= { fmTrapPrefix 401 }

fmTrapRAIDStatusChange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName,
                      fmRAIDStatus, fmRAIDDevIndex }
    STATUS      current
    DESCRIPTION
        "Trap is sent when there is a change in the status of the RAID array, if
present."
    ::= { fmTrapPrefix 402 }

fmTrapLogAlert NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fnGenTrapMsg }
    STATUS      current
    DESCRIPTION
        "Trap is sent when a log based alert has been triggered.
         Alert description included in trap."
    ::= { fmTrapPrefix 403 }
```

```
fmTrapLogRateThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLogRate, fmLogRateThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the incoming log rate has exceeded the threshold"
    ::= { fmTrapPrefix 404 }

fmTrapLogDataRateThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLogDataRate, fmLogDataRateThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the incoming log data rate has exceeded the threshold"
    ::= { fmTrapPrefix 405 }

fmTrapLicGbDayThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLicGbDay, fmLicGbDayThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the used log has exceeded the licensed GB/Day"
    ::= { fmTrapPrefix 407 }

fmTrapLicDevQuotaThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLicDevQuota, fmLicDevQuotaThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the used device quota has exceeded the licensed device
quota"
    ::= { fmTrapPrefix 408 }

fmTrapCpuThresholdExcludeNice NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates that the CPU usage excluding nice processes has exceeded the
threshold"
    ::= { fmTrapPrefix 409 }

--
-- fortinet.fnFortiManagerMib.faModel
--

faModel OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 3 }

faz100 OBJECT IDENTIFIER
    ::= { faModel 1000 }

faz100A OBJECT IDENTIFIER
    ::= { faModel 1001 }

faz100B OBJECT IDENTIFIER
```

```
    ::= { faModel 1002 }

faz100C OBJECT IDENTIFIER
    ::= { faModel 1003 }

faz200D OBJECT IDENTIFIER
    ::= { faModel 2004 }

faz300D OBJECT IDENTIFIER
    ::= { faModel 3004 }

faz400 OBJECT IDENTIFIER
    ::= { faModel 4000 }

faz400B OBJECT IDENTIFIER
    ::= { faModel 4002 }

faz400C OBJECT IDENTIFIER
    ::= { faModel 4003 }

fazvm OBJECT IDENTIFIER
    ::= { faModel 20 }

faz800 OBJECT IDENTIFIER
    ::= { faModel 8000 }

faz800B OBJECT IDENTIFIER
    ::= { faModel 8002 }

faz1000B OBJECT IDENTIFIER
    ::= { faModel 10002 }

faz1000C OBJECT IDENTIFIER
    ::= { faModel 10003 }

faz1000D OBJECT IDENTIFIER
    ::= { faModel 10004 }

faz2000 OBJECT IDENTIFIER
    ::= { faModel 20000 }

faz2000A OBJECT IDENTIFIER
    ::= { faModel 20001 }

faz2000B OBJECT IDENTIFIER
    ::= { faModel 20002 }

faz3000D OBJECT IDENTIFIER
    ::= { faModel 30004 }

faz3000E OBJECT IDENTIFIER
    ::= { faModel 30005 }
```

```
faz3500E OBJECT IDENTIFIER
    ::= { faModel 35005 }

faz4000 OBJECT IDENTIFIER
    ::= { faModel 40000 }

faz4000A OBJECT IDENTIFIER
    ::= { faModel 40001 }

faz4000B OBJECT IDENTIFIER
    ::= { faModel 40002 }

--
-- fortinet.fnFortiManagerMib.fmInetProto
--

fmInetProto OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 4 }

fmInetProtoInfo OBJECT IDENTIFIER
    ::= { fmInetProto 1 }

fmInetProtoTables OBJECT IDENTIFIER
    ::= { fmInetProto 2 }

fmIpSessTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Information on the IP sessions active on the device"
    ::= { fmInetProtoTables 1 }

fmIpSessEntry OBJECT-TYPE
    SYNTAX      FmIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Information on a specific session, including source and destination"
    INDEX       { fmIpSessIndex }
    ::= { fmIpSessTable 1 }

FmIpSessEntry ::= SEQUENCE {
    fmIpSessIndex       FnIndex,
    fmIpSessProto       FmSessProto,
    fmIpSessFromAddr    IpAddress,
    fmIpSessFromPort    InetPortNumber,
    fmIpSessToAddr      IpAddress,
    fmIpSessToPort      InetPortNumber,
    fmIpSessExp         Counter32
}
```

```
fmIpSessIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies
         an IP session within the fmIpSessTable"
    ::= { fmIpSessEntry 1 }

fmIpSessProto OBJECT-TYPE
    SYNTAX      FmSessProto
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The protocol the session is using (IP, TCP, UDP, etc.)"
    ::= { fmIpSessEntry 2 }

fmIpSessFromAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source IP address (IPv4 only) of the session"
    ::= { fmIpSessEntry 3 }

fmIpSessFromPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source port number (UDP and TCP only) of the session"
    ::= { fmIpSessEntry 4 }

fmIpSessToAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination IP address (IPv4 only) of the session"
    ::= { fmIpSessEntry 5 }

fmIpSessToPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination Port number (UDP and TCP only) of the session"
    ::= { fmIpSessEntry 6 }

fmIpSessExp OBJECT-TYPE
    SYNTAX      Counter32
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of seconds remaining before the session expires (if idle)"
    ::= { fmIpSessEntry 7 }

--
-- fortinet.fnFortiManagerMib.fmMibConformance
--

fmMIBConformance OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 10 }

fmTrapsComplianceGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fmTrapHASwitch, fmTrapRAIDStatusChange,
                    fmTrapLogAlert, fmTrapLogRateThreshold,
                    fmTrapLogDataRateThreshold,
                    fmTrapLicGbDayThreshold,
                    fmTrapLicDevQuotaThreshold,
                    fmTrapCpuThresholdExcludeNice }
    STATUS      current
    DESCRIPTION
        "Event notifications"
    ::= { fmMIBConformance 1 }

fmSystemObjectGroup OBJECT-GROUP
    OBJECTS     { fmSysMemUsed, fmSysMemCapacity,
                  fmSysCpuUsage, fmSysDiskCapacity,
                  fmSysDiskUsage, fmSysCpuUsageExcludedNice }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the system status of the device."
    ::= { fmMIBConformance 2 }

fmNotificationObjComplianceGroup OBJECT-GROUP
    OBJECTS     { fmRAIDStatus, fmRAIDDevIndex,
                  fmLogRate, fmLogRateThreshold,
                  fmLogDataRate, fmLogDataRateThreshold,
                  fmLicGbDay, fmLicGbDayThreshold,
                  fmLicDevQuota, fmLicDevQuotaThreshold }
    STATUS      current
    DESCRIPTION
        "Object identifiers used in notifications"
    ::= { fmMIBConformance 3 }

fmSessionComplianceGroup OBJECT-GROUP
    OBJECTS {
        fmIpSessProto,
        fmIpSessFromAddr,
        fmIpSessFromPort,
        fmIpSessToAddr,
        fmIpSessToPort,
```

```
        fmIpSessExp
        }
    STATUS current
    DESCRIPTION "Session related instrumentation"
       ::= { fmMIBConformance 4 }


fmMIBCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
        "The compliance statement for the FortiManager FortiAnalyzer MIB."

    MODULE      -- this module

        GROUP   fmTrapsComplianceGroup
        DESCRIPTION
              "Traps are optional. Not all models support all traps.
                          Consult product literature to see which traps are supported."

        GROUP   fmSystemObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fmNotificationObjComplianceGroup
        DESCRIPTION
                 "Object identifiers used in notifications. Objects are required
                          if their containing trap is implemented."

        GROUP   fmSessionComplianceGroup
        DESCRIPTION
                 "IP session related implementation."

    ::= { fmMIBConformance 100 }

END -- end of module FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.
```

FORTINET

High Performance Network Security